Some examples and graphics depicted herein are provided for illustration only. No real association or connection to ServiceNow products or services is intended or should be inferred.

If you have comments about this documentation, submit your feedback to: docfeedback@servicenow.com
Table of Contents

**Now Platform administration**........................................................................................................................................................................... 7
  Core configuration.......................................................................................................................................................................................... 13
  ServiceNow plugins...................................................................................................................................................................................... 14
  Find components installed with an application.................................................................................................................................. 249
  Using guided setup....................................................................................................................................................................................... 251
  Domain separation and Guided Setup.................................................................................................................................................... 260
  Available system properties................................................................................................................................................................. 261
  Handle HTTP 500 errors........................................................................................................................................................................... 346
  Query join and complexity size limits.................................................................................................................................................... 349
  Web proxy............................................................................................................................................................................................... 349

**Table administration**....................................................................................................................................................................................... 352
  Table extension and classes.................................................................................................................................................................... 352
  Create a table........................................................................................................................................................................................... 355
  Tables module......................................................................................................................................................................................... 360
  Delete a table.......................................................................................................................................................................................... 362
  Delete all records from a table............................................................................................................................................................... 363
  Roll back and delete recovery.............................................................................................................................................................. 365
  Create a table index................................................................................................................................................................................ 370
  Task table............................................................................................................................................................................................... 370
  Data dictionary tables............................................................................................................................................................................ 429
  Schema map for tables.......................................................................................................................................................................... 463
  Create a many-to-many relationship.................................................................................................................................................... 466
  Database views....................................................................................................................................................................................... 467

**List administration**....................................................................................................................................................................................... 481
  List configuration....................................................................................................................................................................................... 481
  Controlling the sort sequence used to display lists............................................................................................................................. 488
  List editor administration...................................................................................................................................................................... 489
  Personal list administration...................................................................................................................................................................... 497
  Administer detail rows........................................................................................................................................................................... 498
  Restrict filters and breadcrumbs with fixed queries......................................................................................................................... 498
  Enable a hierarchical list........................................................................................................................................................................ 503
  Context ranking...................................................................................................................................................................................... 506
  Customize List v2 context menus......................................................................................................................................................... 513
  List v3 administration........................................................................................................................................................................... 519

**Form configuration**....................................................................................................................................................................................... 528
  Using the form designer........................................................................................................................................................................... 528
  Configuring the form layout................................................................................................................................................................. 536

**Form administration**....................................................................................................................................................................................... 551
  Administering form personalization.................................................................................................................................................... 551
  Administering form annotations............................................................................................................................................................... 553
  Administering attachments.................................................................................................................................................................... 553
  Formatters............................................................................................................................................................................................... 559
  Form templates....................................................................................................................................................................................... 575
  UI actions............................................................................................................................................................................................... 587
  UI policies............................................................................................................................................................................................... 595
  Advanced form configuration.............................................................................................................................................................. 599

**Field administration**....................................................................................................................................................................................... 606
  Field types............................................................................................................................................................................................... 606
  Add and customize a field in a table...................................................................................................................................................... 716
  Field normalization and transformation.................................................................................................................................................... 735
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data policy</td>
<td>775</td>
</tr>
<tr>
<td>Data lookup and record matching support</td>
<td>783</td>
</tr>
<tr>
<td>State Management</td>
<td>789</td>
</tr>
<tr>
<td>Add a state model and transitions</td>
<td>790</td>
</tr>
<tr>
<td>Implement process flow and UI actions with a state model</td>
<td>792</td>
</tr>
<tr>
<td>Installed with State Model</td>
<td>792</td>
</tr>
<tr>
<td>Currency administration</td>
<td>793</td>
</tr>
<tr>
<td>Setting up and operating standard currency fields</td>
<td>794</td>
</tr>
<tr>
<td>Setting up and operating FX Currency fields</td>
<td>806</td>
</tr>
<tr>
<td>System localization</td>
<td>822</td>
</tr>
<tr>
<td>Define locales</td>
<td>822</td>
</tr>
<tr>
<td>Language internationalization support</td>
<td>823</td>
</tr>
<tr>
<td>Localize price fields</td>
<td>836</td>
</tr>
<tr>
<td>Localization settings</td>
<td>837</td>
</tr>
<tr>
<td>Custom translations</td>
<td>839</td>
</tr>
<tr>
<td>Localization Framework</td>
<td>857</td>
</tr>
<tr>
<td>Activation of Localization Framework</td>
<td>857</td>
</tr>
<tr>
<td>Localization Framework Roles</td>
<td>859</td>
</tr>
<tr>
<td>Artifact configuration</td>
<td>860</td>
</tr>
<tr>
<td>Localization Framework Settings</td>
<td>867</td>
</tr>
<tr>
<td>Request Translations UI</td>
<td>882</td>
</tr>
<tr>
<td>Localization task states</td>
<td>885</td>
</tr>
<tr>
<td>Translation modes</td>
<td>886</td>
</tr>
<tr>
<td>Fulfill a localization task</td>
<td>886</td>
</tr>
<tr>
<td>Approve a localization task</td>
<td>888</td>
</tr>
<tr>
<td>Error messages in the Localization Framework</td>
<td>888</td>
</tr>
<tr>
<td>Localization Insights dashboard</td>
<td>891</td>
</tr>
<tr>
<td>Dynamic Translation</td>
<td>895</td>
</tr>
<tr>
<td>Activation of Dynamic Translation</td>
<td>895</td>
</tr>
<tr>
<td>DynamicTranslation API</td>
<td>897</td>
</tr>
<tr>
<td>Microsoft Azure Translator Service spoke</td>
<td>898</td>
</tr>
<tr>
<td>IBM Watson Translator Service spoke</td>
<td>902</td>
</tr>
<tr>
<td>Google Cloud Translator Service spoke</td>
<td>905</td>
</tr>
<tr>
<td>Dynamic Translation spoke</td>
<td>911</td>
</tr>
<tr>
<td>Language Detection spoke</td>
<td>913</td>
</tr>
<tr>
<td>Integrate with a translation service provider</td>
<td>914</td>
</tr>
<tr>
<td>Migrate to version v3 of a translator configuration</td>
<td>917</td>
</tr>
<tr>
<td>Limitations in Dynamic Translation</td>
<td>919</td>
</tr>
<tr>
<td>Dynamic translation on forms and activity streams</td>
<td>920</td>
</tr>
<tr>
<td>Translate a knowledge article</td>
<td>922</td>
</tr>
<tr>
<td>Dynamic Translation for Agent Chat Overview</td>
<td>924</td>
</tr>
<tr>
<td>Domain separation and Dynamic Translation</td>
<td>924</td>
</tr>
<tr>
<td>Time configuration</td>
<td>929</td>
</tr>
<tr>
<td>Date and Date/Time fields</td>
<td>930</td>
</tr>
<tr>
<td>Time zones</td>
<td>937</td>
</tr>
<tr>
<td>Creating business calendars</td>
<td>940</td>
</tr>
<tr>
<td>Defining fiscal calendars</td>
<td>958</td>
</tr>
<tr>
<td>Creating and using schedules</td>
<td>961</td>
</tr>
<tr>
<td>System scheduler</td>
<td>981</td>
</tr>
<tr>
<td>Viewing record information over time</td>
<td>1000</td>
</tr>
<tr>
<td>Client transaction timings</td>
<td>1022</td>
</tr>
<tr>
<td>Search administration</td>
<td>1028</td>
</tr>
<tr>
<td>Machine learning solutions for Search administration</td>
<td>1029</td>
</tr>
<tr>
<td>Features of Search administration</td>
<td>1030</td>
</tr>
<tr>
<td>Search Suggestions</td>
<td>1030</td>
</tr>
<tr>
<td>Search signals</td>
<td>1038</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Zing text indexing and search engine</td>
<td>1040</td>
</tr>
<tr>
<td>AI Search</td>
<td>1112</td>
</tr>
<tr>
<td>Contextual search</td>
<td>1229</td>
</tr>
<tr>
<td>CMDB Search</td>
<td>1288</td>
</tr>
<tr>
<td>Events</td>
<td>1290</td>
</tr>
<tr>
<td>Event registry</td>
<td>1291</td>
</tr>
<tr>
<td>Event states</td>
<td>1291</td>
</tr>
<tr>
<td>Event logs</td>
<td>1292</td>
</tr>
<tr>
<td>The incident events business rule</td>
<td>1293</td>
</tr>
<tr>
<td>Sample scripts from the change events business rule</td>
<td>1294</td>
</tr>
<tr>
<td>Script actions</td>
<td>1295</td>
</tr>
<tr>
<td>Global events</td>
<td>1298</td>
</tr>
<tr>
<td>Create an event</td>
<td>1299</td>
</tr>
<tr>
<td>Register an event</td>
<td>1300</td>
</tr>
<tr>
<td>Reprocess an event</td>
<td>1301</td>
</tr>
<tr>
<td>Pass event parameters from a workflow to a notification</td>
<td>1301</td>
</tr>
<tr>
<td>Data management</td>
<td>1301</td>
</tr>
<tr>
<td>Unique record identifier (sys_id)</td>
<td>1304</td>
</tr>
<tr>
<td>Data archiving</td>
<td>1305</td>
</tr>
<tr>
<td>Export and import XML files</td>
<td>1330</td>
</tr>
<tr>
<td>Export sets</td>
<td>1354</td>
</tr>
<tr>
<td>Import sets</td>
<td>1361</td>
</tr>
<tr>
<td>System clone</td>
<td>1512</td>
</tr>
<tr>
<td>Database clone</td>
<td>1538</td>
</tr>
<tr>
<td>Domain separation and Data Management</td>
<td>1541</td>
</tr>
<tr>
<td>Integration with third-party applications and data sources</td>
<td>1541</td>
</tr>
<tr>
<td>Integration options</td>
<td>1542</td>
</tr>
<tr>
<td>User administration</td>
<td>1578</td>
</tr>
<tr>
<td>Manage user administration system properties</td>
<td>1578</td>
</tr>
<tr>
<td>Add a new company</td>
<td>1580</td>
</tr>
<tr>
<td>Add a department</td>
<td>1581</td>
</tr>
<tr>
<td>Create a user</td>
<td>1581</td>
</tr>
<tr>
<td>User self-registration</td>
<td>1586</td>
</tr>
<tr>
<td>Impersonate a user</td>
<td>1587</td>
</tr>
<tr>
<td>Manage user sessions</td>
<td>1589</td>
</tr>
<tr>
<td>Groups</td>
<td>1591</td>
</tr>
<tr>
<td>Roles</td>
<td>1595</td>
</tr>
<tr>
<td>Non-interactive sessions</td>
<td>1612</td>
</tr>
<tr>
<td>Instance Usage</td>
<td>1614</td>
</tr>
<tr>
<td>Authentication</td>
<td>1618</td>
</tr>
<tr>
<td>Normalization Data Services</td>
<td>1848</td>
</tr>
<tr>
<td>Metrics</td>
<td>1851</td>
</tr>
<tr>
<td>Create a metric</td>
<td>1851</td>
</tr>
<tr>
<td>Sample field value duration script</td>
<td>1852</td>
</tr>
<tr>
<td>Metric instance</td>
<td>1853</td>
</tr>
<tr>
<td>Platform performance</td>
<td>1855</td>
</tr>
<tr>
<td>Transaction log response times</td>
<td>1855</td>
</tr>
<tr>
<td>Network response times</td>
<td>1858</td>
</tr>
<tr>
<td>Browser settings and performance</td>
<td>1860</td>
</tr>
<tr>
<td>Diagnostics page</td>
<td>1860</td>
</tr>
<tr>
<td>System Diagnostics Stats Tools</td>
<td>1864</td>
</tr>
<tr>
<td>Use a slow query log</td>
<td>1867</td>
</tr>
<tr>
<td>Index suggestions for slow queries</td>
<td>1869</td>
</tr>
<tr>
<td>Transaction call chains</td>
<td>1888</td>
</tr>
<tr>
<td>Transaction cancellation</td>
<td>1893</td>
</tr>
<tr>
<td>Import set performance</td>
<td>1895</td>
</tr>
</tbody>
</table>
**Now Platform administration**

The Now Platform® is an application platform as a service that automates business processes across the enterprise. The Now Platform provides the infrastructure to help your organization develop, run, and manage applications.
**Provide a single system of engagement for the enterprise**

Use the Now Platform to deliver a common set of core capabilities and reusable components to the entire enterprise rather than individual departments or functions. Use the core capabilities to eliminate data silos by sharing information within a single data model. Extend the data model with a flexible table schema and reusable components.

View and download the full infocard for a highlight of Now Platform administration features.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Deliver a common set of core capabilities</strong></td>
<td>Provide users with high-performance business services that make work simpler, faster, and more productive.</td>
</tr>
<tr>
<td><strong>Eliminate silos with a single data model</strong></td>
<td>Prevent silos by sharing data across the enterprise from your instance. Extend the data model with a flexible table schema.</td>
</tr>
<tr>
<td><strong>Provide reliable and secure cloud services</strong></td>
<td>Provide reliable service from multi-instance cloud services. Secure data and communications with encryption.</td>
</tr>
</tbody>
</table>
Deliver a common set of core capabilities

The Now Platform supports your apps, business requirements, and workflows. With the Now Platform, you can configure global settings for the entire platform or specific applications.
Eliminate silos with a single data model
With the Now Platform, you can eliminate silos by sharing data between applications and departments. You can also configure and extend your data model with a flexible table schema.
Provide reliable and secure cloud services
The Now Platform meets your performance, reliability, privacy, and compliance requirements. With the cloud services of the Now Platform, you can ensure that your data is always secure, with each new release offering new security properties.

Get started

- Learn about the Now Platform architecture. See this video:
- Learn about tables, records, and fields. See this video:
- Learn about upgrades and conversions. See Upgrades and conversions

Applications and features

- Core configuration
- Currency administration
- Data management
- Domain separation
- Dynamic Translation
- Events
- Field administration
- Form administration
- Form configuration
- Integrate with third-party applications and data sources
- List administration
- Metrics
- Platform performance
- Platform security
- Search administration
- State Management
- System localization
- Table administration
- Time configuration
- Upgrades and conversions
- User administration

Core configuration

Core configuration encompasses changes made to the platform as well as supporting applications. These changes can affect global settings as well as settings for particular applications.

These settings include:

- Form administration and lists: change the behavior and appearance of forms and lists.
- Navigation and UI and search: configure how users browse and search in the platform.
- Time and performance: keep your organization running and on time.
- Localization and mobile device support: take the platform anywhere.
- Plugins and out-of-box appendix: expand the platform to fit your needs.
ServiceNow plugins

Plugins are software components that provide specific features and functionalities within a ServiceNow instance.

Activating plugins

If a plugin is not active by default on the Now Platform, you can activate it from the All Applications list in your instance. For more information, see Activate a plugin.

If you cannot find a plugin in the All Applications list for activation, the plugin may require activation by ServiceNow personnel. To get a plugin activated by ServiceNow personnel, follow the steps in Request a plugin.

Some plugins require a paid subscription before activation. To purchase a subscription, contact your ServiceNow account manager. When you purchase a subscription, certain plugins are activated automatically. If a paid plugin isn't activated automatically, you can manually activate it from the All Applications list in your instance. If the plugin doesn't appear in the instance, submit a request via the Now Support Service Catalog.

For more information on plugins that are associated with paid subscriptions, see View subscription applications and plugins.

**Note:** After a plugin is activated, you cannot disable or deactivate it. If needed, you can hide the functionality. You should thoroughly test, in a non-production instance, the specific features and functionalities that are installed when you activate the plugin before using them in a production instance.

Relationships between plugins

Some plugins depend on other plugins being activated.

Sometimes, a plugin cannot work at all unless one or more other plugins are installed. When you activate a plugin with dependent plugins, the system notifies you of the dependencies before it completes the activation. If you opt to continue with activation, the system automatically activates all the plugins required.

In other cases, the plugin works, but certain features that do not apply to your system are not installed. When you ask to activate a plugin in this category, the system notifies you of the dependencies before it completes the activation. If you opt to continue, the system activates the requested plugin but does not include the features that depend on other plugins.

Personal developer instances

You can test a plugin on your personal developer instance (PDI) before launching it in a production instance. If a plugin isn't active by default on a PDI, you can activate the plugin without requesting or purchasing it.

To activate a plugin on a PDI, use the All Applications page on your instance. If the plugin isn't available on the All Applications page, activate it from the . For more information, see Activate a plugin on a personal developer instance.

**Note:** Some plugins aren't available for activation on PDIs.

Activate a plugin

You can activate most plugins to expand features and functionalities in the Now Platform.

Role required: admin

1. Navigate to System Applications > All Available Applications > All.
2. Find the plugin using the filter criteria and search bar. You can search for the plugin by its name or ID. If you cannot find a plugin, you might have to request it from ServiceNow personnel. For more information, see Request a plugin.

3. Click Install, and then in the Activate Plugin dialog box, click Activate.

**Note:** When domain separation and delegated admin are enabled in an instance, the administrative user must be in the global domain. Otherwise, the following error appears: Application installation is unavailable because another operation is running: Plugin Activation for <plugin name>.

### Activate a plugin on a personal developer instance

You can test a plugin on your personal developer instance (PDI) before launching it in a production instance.

Request a PDI on the ServiceNow® Developer Site.

If a plugin isn't active by default on a PDI, you can activate the plugin without requesting or purchasing it.

To activate a plugin on a PDI, use the All Applications page on your instance. If the plugin isn't available on the All Applications page, activate it from the .

**Note:** Some plugins aren't available for activation on PDIs.

Activate the plugin from the All Applications page or the Developer Site.

<table>
<thead>
<tr>
<th>Activation method</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Applications page</td>
<td>In your PDI, navigate to System Applications &gt; All Available Applications &gt; All. Find the plugin and then activate it.</td>
</tr>
<tr>
<td></td>
<td>For more information on using the All Applications page, see Activate a plugin.</td>
</tr>
<tr>
<td>Activation method</td>
<td>Procedure</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------</td>
</tr>
</tbody>
</table>
| Developer Site    | **a.** Sign in to the ServiceNow® Developer Site.  
**b.** On the home page, go to the Instance Management widget and select **Manage > Activate plugin.**  
The Instance Management widget is titled **Your Instance.** It contains information such as the status, URL, and release version of your PDI. |
|                   | **c.** On the window, locate the plugin to activate.  
**d.** Next to the plugin listing, select **Activate.**  
If available, you can further select to activate the plugin only or include demo data. |

---

**Your Instance**

<table>
<thead>
<tr>
<th>INSTANCE STATUS</th>
<th>Activate plugin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online</td>
<td>Release instance</td>
</tr>
<tr>
<td>INSTANCE URL</td>
<td>Remove demo data</td>
</tr>
<tr>
<td><a href="https://devtest35592.service-now">https://devtest35592.service-now</a></td>
<td>Reset admin password</td>
</tr>
<tr>
<td>RELEASE</td>
<td>Reset and wipe instance</td>
</tr>
<tr>
<td>Madrid</td>
<td>Upgrade instance</td>
</tr>
<tr>
<td>REMAINING INACTIVITY</td>
<td>Manage</td>
</tr>
<tr>
<td>10 days</td>
<td></td>
</tr>
</tbody>
</table>

Refresh Status...
Request a plugin

If a plugin does not appear on the All Applications page, you cannot activate it yourself. Request activation of the plugin by ServiceNow personnel.

Role required: admin

There are two ways to request a plugin:

• Access the Now Support Service Catalog directly by clicking Service Catalog > Activate Plugin on Now Support.
• Access the Now Support Service Catalog through the All Applications page on your instance by following these steps.

Watch this one-minute video to learn more about using the HI Service Catalog to request plugins.

1. Navigate to System Applications > All Available Applications > All.
2. On the All Applications page, click **Request Plugin** to open the Request form on HI.
3. On Now Support, select the redirect link to access the Now Support Service Portal Service Catalog.

<table>
<thead>
<tr>
<th>Activate Plugin</th>
</tr>
</thead>
<tbody>
<tr>
<td>In order to enhance the user experience, we have redesigned Activate a Plugin service catalog. Please use the new HI Service Portal 'Activate a Plugin' service catalog item. You can also use Manage Instances page on Service Portal to Activate a Plugin.</td>
</tr>
<tr>
<td>Take me to the HI Service Portal Activate a Plugin Service Catalog.</td>
</tr>
</tbody>
</table>

4. On the form, fill in the fields.

**Activate Plugin request form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Instance</td>
<td>Instance on which to activate the plugin.</td>
</tr>
<tr>
<td>Plugin Name</td>
<td>Name of the plugin to activate.</td>
</tr>
<tr>
<td>Specify the date and time you would like this plugin to be enabled</td>
<td>The date and time must be at least two business days from the current time.</td>
</tr>
</tbody>
</table>

**Note:** Plugins are activated in two batches, once in the morning and once in the evening, on every business day in the US Pacific time zone. If the plugin must be activated at a specific time, enter the request in the **Reason/Comments** field.

| Reason/Comments | Information that would be helpful for the ServiceNow personnel who are activating the plugin. For example, if you need the plugin activated at a specific time instead of during one of the default activation windows, specify that in the comments. |

5. Click **Submit**.

**List of plugins (Quebec)**

List of all plugins that you can activate if you have the admin role.

If a plugin does not appear on this list, it may require activation by ServiceNow personnel. Request these plugins through the Now Support Customer Service System instead of activating them yourself.

- For steps on activating a plugin yourself, see **Activate a plugin**.
- For steps on requesting a plugin that you cannot activate yourself, see **Request a plugin**.

**Note:** For a list of all new and changed plugins for this release, see Changes to plugins in the Quebec release.
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action Status Automation</td>
<td>com.sn_action_status</td>
<td>This plugin tracks blocking records created for tasks and updates the action status indicators on the task list.</td>
<td>Active</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>Activity formatter</td>
<td>com.glide.ui_activity_formatter</td>
<td>This plugin lets you quickly and easily filter the list of activities, or history, on a task form.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Advanced Work Assignment</td>
<td>com.glide.awa</td>
<td>Automatically assigns work items to agents based on their availability, capacity, and skills.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.skills_management</td>
</tr>
<tr>
<td>Advanced Work Assignment - Agent Affinity</td>
<td>com.glide.awa.agent_affinity</td>
<td>Enable work assignment to the best-suited agent based on the agent’s affinity to the work item.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.awa</td>
</tr>
<tr>
<td>Advanced Work Assignment for HRSD</td>
<td>com.sn_hr.awa</td>
<td>Contains out of box configuration data supporting routing, queuing, and assignment of HRSM cases, chats and calls to agents.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.awa, com.sn_hr_core, com.glide.interaction.awa</td>
</tr>
<tr>
<td>Advanced Work Assignment for Incidents</td>
<td>com.snc.incident.awa</td>
<td>Default configuration to support Advanced Work Assignment for Incident</td>
<td>Active</td>
<td>false</td>
<td>com.glide.awa, com.snc.agent_workspace.itsm</td>
</tr>
<tr>
<td>Agent Chat</td>
<td>com.glide.interaction.awa</td>
<td>Enables Workspace Agent Chat and the Chat service channel in Advanced Work Assignment.</td>
<td>Active</td>
<td>true</td>
<td>com.glide.interaction, com.glide.awa</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Agent Client Collector</td>
<td>sn_agent</td>
<td>Management of Agent Client Collector</td>
<td>Active</td>
<td>false</td>
<td>• com.snc.sa.mid.webserver</td>
</tr>
<tr>
<td>Framework New in Quebec</td>
<td></td>
<td>(Available in the ServiceNow Store)</td>
<td></td>
<td></td>
<td>• com.snc.cmdb.scoped</td>
</tr>
<tr>
<td>Agent Client Collector</td>
<td>sn_itmon</td>
<td>Monitoring solution using the Agent Client Collector</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Monitoring New in Quebec</td>
<td></td>
<td>(Available in the ServiceNow Store)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent Forecast</td>
<td>com.sn_agent_forecast</td>
<td>Forecasts agents based on historical data.</td>
<td>false</td>
<td></td>
<td>com.snc.clotho</td>
</tr>
<tr>
<td>(New in Quebec)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent Intelligence</td>
<td>com.glide.platform_ml</td>
<td>Renamed to Predictive Intelligence.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.platform_ml_pa</td>
</tr>
<tr>
<td>Reports</td>
<td>com.glide.platform_ml_pa</td>
<td>Renamed to Predictive Intelligence Reports.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Agent Schedule</td>
<td>com.snc.agent_schedule</td>
<td>Enables customer service agents and field service technicians to see work schedules and assignments and also add personal events such as meetings or appointments.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.app.agent_calendar_widget</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Agent Workspace</td>
<td>com.agent_workspace</td>
<td>It is a suite of tools that provide agents, case managers, help desk</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.uxbuilder</td>
</tr>
<tr>
<td></td>
<td></td>
<td>professionals, and managers with tools to help answer customer questions</td>
<td></td>
<td></td>
<td>• com.glide.graphql</td>
</tr>
<tr>
<td></td>
<td></td>
<td>or resolve customer problems.</td>
<td></td>
<td></td>
<td>• com.glide.interaction</td>
</tr>
<tr>
<td>Agent Workspace - Knowledge</td>
<td>sn-component-workspace-knowledge</td>
<td>Enables use of Knowledge Base in Agent Assist.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.agent_workspace.config</td>
</tr>
<tr>
<td>Agent Workspace - List</td>
<td>com.snc.agent_workspace.list</td>
<td>Workspace List Configurations</td>
<td>Active</td>
<td>false</td>
<td>com.snc.agent_workspace.config</td>
</tr>
<tr>
<td>Agent Workspace - Ribbon</td>
<td>com.snc.agent_workspace.ribbon</td>
<td>Workspace Ribbon Configurations</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.uxbuilder</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Provides SOAP Access to GlideAggregate functionality.</td>
<td></td>
<td></td>
<td>• com.snc.agent_workspace.config</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.sn_resolutionshaper</td>
</tr>
<tr>
<td>Aggregate Web Service</td>
<td>com.glide.web_service_aggregate</td>
<td>Provides SOAP Access to GlideAggregate functionality.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Agile Development 2.0</td>
<td>com.snc.sdlc.agile.2.0</td>
<td>The Agile Development 2.0 plugin provides enhanced functionality on top of</td>
<td>Active</td>
<td>true</td>
<td>• com.snc.sdlc.scrum.ppm_int</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Agile Development. If you already have a customized version of Agile</td>
<td></td>
<td></td>
<td>• com.snc.planned_task_v2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Development, delete the customizations before activating Agile Development</td>
<td></td>
<td></td>
<td>• com.snc.sdlc.agile.2.0.common</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.0 to ensure that all features work properly. Refer to the documentation</td>
<td></td>
<td></td>
<td>• com.snc.sdlc.ranking</td>
</tr>
<tr>
<td></td>
<td></td>
<td>for detailed steps to delete the customizations.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
</table>
| Agile Development — Unified Backlog       | com.snc.sdlc.agile.multi_task | Enables you to maintain a centralized backlog containing records of different task types, such as defects, problems, incident tasks, and stories. Include any tasks into your agile workflow | Active | false          | • com.snc.sdlc.agile.2.0  
• com.snc.sdlc.agile.multi_task.common |
| Agile - Scaled Agile Framework - Essential SAFe | com.snc.sdlc.safe     | Scaled Agile Framework was designed to apply Lean-Agile principles to the entire organization. Essential SAFe is most basic configuration of the framework and it provides the minimal elements necessary to be successful with SAFe: manage your agile release train backlog, plan program increments, | Active | true           | • com.snc.sdlc.ranking  
• com.snc.sdlc.agile.2.0 |
| Agile - Scaled Agile Framework - Portfolio SAFe | com.snc.sdlc.portfolio_safe | Use Portfolio SAFe to apply lean and agile principles to your portfolio work.                          | Active | true           | • com.snc.sdlc.safe  
• com.snc.portfolio_management |
| Agile Development 2.0 - ATF Tests         | com.snc.sdlc.agile.2.0.atf | Agile Development 2.0 - ATF Tests provides you test cases and test suites that can be run on the Agile Development 2.0 application. | Active | false          |                                                        |
| AI Search (New in Quebec)                 | com.glide.ais           | Installs and enables AI Search capabilities, providing relevant, contextual, and personal search experiences across different interfaces. | Active | false          | • com.glide.search.signal_data  
• com.glide.platform_ml  
• com.glide.nlu  
• com.snc.nlu_studio |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI Search Assist</td>
<td>com.snc.ai_search_assist</td>
<td>Helps users deflect or quickly resolve their issues without involving the service desk operators. It can include results from Knowledge and Service catalog, allowing a user to directly order a catalog item from a search.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.search</td>
</tr>
<tr>
<td>Alert Intelligence</td>
<td>com.em-scoped-app</td>
<td>This plugin is part of the Event Management application. It contains content for the Alert Intelligence workspace.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
</tbody>
</table>
| Analytics Center         | com.snc.pa.analytics_center| Performance Analytics Center - Enables users to get answers about their data quickly using search-driven analytics. | Inactive| false          | • com.agent_workspace  
• com.workspace_core  
• sn-component-nlq  
• com.snc.par.nlq.core |
| Analytics Task           | com.snc.pa.analytics_task| Provides the core framework for workflow related to Analytics. It consists of the analytics task table and related artifacts. | Active| false          |                                      |
| Angular AMB Services     | com.glide.ui.ng.amb     | Angular Services for AMB                                                     | Active| false          | • com.glide.ui.ng  
• com.glide.amb  
• com.glide.record_watcher |
| Anonymous Connect Support| com.glide.connect.anonymous_support| Plugin to enable access and properties for Anonymous Connect Support.         | Inactive| false          | com.glide.connect.support          |
| API Analytics            | com.glide.api_analytics | Allows admins to view API Analytics statistics for web services.              | Active| false          | • com.glide.db.query_stats  
• com.snc.pa  
• com.glideapp.canvas                  |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>API Stats</td>
<td>com.glide.stats.api</td>
<td>API Stats</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.db.query_stats</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.pa</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glideapp.canvas</td>
</tr>
<tr>
<td>App APIs</td>
<td>com.glide.app_api</td>
<td>APIs for fetching Application and Application Rollback related information.</td>
<td>Active</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>App Dependency Client</td>
<td>com.sn_dependentclient</td>
<td>Plugin to provide list of store applications/integrations based on their active plugins. Uses store's web service to create a cache of such applications on the customer instances itself.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>App Engine Studio</td>
<td>com.snc.app-engine-studio</td>
<td>Installs and enables App Engine Studio, a development tool for creators of varying skill levels to build applications that meet the immediate needs of your organization.</td>
<td>Inactive</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>Application Authorization</td>
<td>com.glide.sys.app_authorization</td>
<td></td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Application Creator</td>
<td>com.snc.apps_creator</td>
<td>Retired. Replaced by the Platform as a Service plugin.</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.ui.angular</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.ui.heisenberg</td>
</tr>
<tr>
<td>Application Creator Templates</td>
<td>com.snc.apps_creator_template</td>
<td>Hosts system application creator templates.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Application Design Restrictions</td>
<td>com.glide.scope.design</td>
<td>System for restricting and capturing tables augmented by an application</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Application Diagnostics Tool</td>
<td>com.snc.app_diagnostics_tool</td>
<td>Helps you to diagnose the PPM Applications, with quick diagnostic scans and resolve the issues with fix scripts.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Application File</td>
<td>com.snc.apps_file</td>
<td>Associates configuration records with an application and tracks record metadata.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Application Metadata</td>
<td>com.snc.metadata</td>
<td>Adds relationships and UI actions to work with metadata.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>-------------------------------------------------------------------</td>
</tr>
<tr>
<td>Application Portfolio Management</td>
<td>com.snc.apm</td>
<td>Helps enterprises have visibility into their business applications inventory and enables analysts to rationalize business applications. Provides Performance Analytics dashboards like Application 360, Landscape Analysis, and associated dashboards of Business Applications with Change requests, Incidents, and Problems. This plugin activates the following related plugins if they are not already active:</td>
<td>Active</td>
<td>true</td>
<td>• com.snc.certification_v2 • com.snc.fiscal_calendar • com.snc.treemap • com.snc.sp_workbench_widgets • com.snc.apm.business_planner • com.snc.pa.apm • com.snc.demand_core • com.snc.apm.predictive_intelligence</td>
</tr>
<tr>
<td>Application Portfolio Management – Predictive Intelligence</td>
<td>com.snc.apm.predictive_intelligence</td>
<td>predicts application category by applying algorithms like similarity on business applications related data.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Portfolio Management – ATF Test</td>
<td>com.snc.apm.atf</td>
<td>Validates ATF tests for Application Portfolio Management</td>
<td>Active</td>
<td>false</td>
<td>com.snc.apm</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Application Portfolio Management Core</td>
<td>com.snc.apm_core</td>
<td>Enables register a new business application</td>
<td>Active</td>
<td>false</td>
<td>com.glideapp.servicecatalog.platform</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>com.glide.hub.designer_backend.model</td>
</tr>
<tr>
<td>Application Service</td>
<td>com.snc.cmdb.it_service</td>
<td>Provides functionality and view for Application Service creation, editing and history view.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.itom.ui</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>com.snc.cmdb</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>com.snc.cmdb.service.modeling</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>com.glide.ui.list_v3_components</td>
</tr>
<tr>
<td>Applications Access Control</td>
<td>com.snc.apps_access</td>
<td>Implements file-level access for application development.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.apps</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>com.snc.apps_picker</td>
</tr>
<tr>
<td>Applications Picker</td>
<td>com.snc.apps_picker</td>
<td>Allows users to select the desired application during application development.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Apply Once APIs</td>
<td>com.glide.system_apply_once</td>
<td>APIs for altering the behavior of any 'apply_once' update in a plugin during plugin activation/upgrade</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Appointment Booking</td>
<td>com.snc.appointment_booking</td>
<td>Enables customers to book service appointments from the Customer and Consumer Service Portals.</td>
<td>Inactive</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>Appointment Booking Demo Data</td>
<td>com.snc.appointment_booking</td>
<td>Provides demo data for the appointment booking feature.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Approvals with e-Signature</td>
<td>com.glide.e_signature_appro</td>
<td>Adds a prompt for credentials when an approver attempts to approve a request via the list context menu or Approve UI Action on the Approval form.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Architecture Compliance</td>
<td>com.snc.architecture_compliance</td>
<td>Manages scheduled or on-demand audits of CMDB records, to determine if configuration items (CI) match expected attributes.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.certification_core</td>
</tr>
<tr>
<td>Assessment</td>
<td>com.snc.assessment_core</td>
<td>Provides capabilities to use custom questionnaires and scripted queries to evaluate, score, and compare any records in ServiceNow.</td>
<td>Active</td>
<td>true</td>
<td>com.glideapp.workflow, com.glideapp.survey, com.snc.bestpractice.task_survey, com.glide.survey_designer</td>
</tr>
<tr>
<td>Assessment Designer</td>
<td>com.glide.assessment_designer_common</td>
<td>Activates assessment designer that is a drag-and-drop interface to create assessments.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.assessment_designer.common</td>
</tr>
<tr>
<td>Assessment Designer Common</td>
<td>com.glide.assessment_designer_common</td>
<td>Base plugin for assessment related designers like Quiz Designer, Survey Designer, Assessment designer. You must activate Assessment Designer Common plugin before using Quiz Designer, Survey Designer, or Assessment Designer. By default, this plugin is activated.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.ui.ng.de</td>
</tr>
<tr>
<td>Asset Management</td>
<td>com.snc.asset_management</td>
<td>Lets you manage all your assets, consumables, and software licenses.</td>
<td>Active</td>
<td>true</td>
<td>com.snc.expense_line, com.snc.model, com.snc.organization_management, com.snc.fixed_asset, com.snc.depreciation, com.snc.automation, com.glideapp.home</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Assignment Workbench</td>
<td>com.snc.assignment_workbench</td>
<td>Provides a workbench that customer service managers can use to evaluate agents based on configurable criteria, such as skills and availability, and then assign tasks to the desired agents.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.matching_rule</td>
</tr>
<tr>
<td>Auto Recovery</td>
<td>com.glide.autorecovery</td>
<td>Enables Auto Recovery functionality.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Automated Test Framework</td>
<td>com.glide.automated_testing</td>
<td>provides ATF steps that validate access to the application navigator.</td>
<td>Active</td>
<td>true</td>
<td>com.glide.rollback, com.glide.ui.angular, com.glide.element_mapping, com.glide.vars</td>
</tr>
<tr>
<td>Automated Test Framework - Application Navigator</td>
<td>com.glide.automated_testing</td>
<td>Provides ATF steps that validate access to the application navigator.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.automated_testing.framework</td>
</tr>
<tr>
<td>Automated Test Framework - Custom UI</td>
<td>com.glide.automated_testing</td>
<td>Provides ATF steps that validate access to the application navigator.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.automated_testing.framework</td>
</tr>
<tr>
<td>Automated Test Framework - Parameters</td>
<td>com.glide.automated_testing</td>
<td>Provides ATF steps that validate access to the application navigator.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.automated_testing.framework</td>
</tr>
<tr>
<td>Automated Test Framework - Reporting</td>
<td>com.glide.automated_testing</td>
<td>Provides ATF steps that validate access to the application navigator.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.automated_testing.framework</td>
</tr>
<tr>
<td>Automated Test Framework - REST Inbound</td>
<td>com.glide.automated_testing</td>
<td>Provides ATF steps that validate access to the application navigator.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.automated_testing.framework</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-----------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Automated Test Framework - Schedule</td>
<td>com.glide.automated_testing_impl.schedule</td>
<td>Scheduling automated tests.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.automated_testing_framework</td>
</tr>
<tr>
<td>Automated Test Framework - Allowlist Client Errors</td>
<td>com.glide.automated_testing_impl.script</td>
<td>Errors found during UI test execution can be ignored or tracked as warnings. Test designers can complete their work while developers investigate and resolve scripting issues.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.automated_testing_framework</td>
</tr>
<tr>
<td>Automated Test Framework Service Catalog</td>
<td>com.glide.automated_testing_impl.service_catalog</td>
<td>Framework Service Catalog test step configuration.</td>
<td>Active</td>
<td>true</td>
<td>com.glide.automated_testing_framework, com.glideapp.servicecatalog</td>
</tr>
<tr>
<td>Automated Test Framework Service Portal</td>
<td>com.glide.automated_testing_impl.service_portal</td>
<td>Framework Service Portal test step configuration. This plugin can only be activated by activating the &quot;Service Portal - Core&quot; plugin.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.automated_testing_framework</td>
</tr>
<tr>
<td>Automated Test Scripts For Survey</td>
<td>com.glide.automated_testing_impl.survey</td>
<td>Automated Test Scripts For Survey.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.automated_testing_framework, com.snc.assessment_core</td>
</tr>
<tr>
<td>Automatic Assignment</td>
<td>com.snc.automatic_assignment</td>
<td>Allows any application that uses tables that are children of Task [task] to use auto-assignment to automatically find eligible assignees for any task.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>AWA Channel Management</td>
<td>com.sn_channel_management</td>
<td>AWA Channel Management: main plugin which supports various functionalities for AWA Service Channels and Queues under Manager Workspace</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.awa</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.wfo</td>
</tr>
<tr>
<td>Badge Reader Integration</td>
<td>com.snc.badge_reader</td>
<td>Badge Reader Integration Framework which allows other applications to integrate with badge reader hardware.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Base Upgrade Logger</td>
<td>com.glide.base_upgrade_logger</td>
<td></td>
<td>Active</td>
<td>false</td>
<td>• com.glide.ui.mergetool</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.ui.diagnostics</td>
</tr>
<tr>
<td>Basic Export Set Functionality</td>
<td>com.glide.system_export_set</td>
<td></td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Benchmark Client</td>
<td>com.sn_bm_client</td>
<td>Benchmark Insights for Customers.</td>
<td>Active</td>
<td>false</td>
<td>com.sn_bm_common</td>
</tr>
<tr>
<td>Benchmark Common</td>
<td>com.sn_bm_common</td>
<td>Common code for Benchmark Insights.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Benchmarks Spoke</td>
<td>com.sn_bm_client.spoke</td>
<td>Contains the evaluation framework for Benchmarks Recommendations.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.hub</td>
</tr>
<tr>
<td>Best Practice - Bulk CI Changes</td>
<td>com.snc.bestpractice.bulkchange</td>
<td>This plugin is intended to be used with the legacy Change Management state models which were used prior to the Geneva release. It allows CMDB updates to be proposed and applied to one or more in scope configuration items as part of your change management process.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------</td>
<td>----</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Best Practice - Change Risk Calculator</td>
<td>com.snc.bestpractice.change</td>
<td>Simple risk and impact calculations for change management.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Best Practice - Incident Resolution Workflow</td>
<td>com.snc.bestpractice.incident</td>
<td>Best practices for incident resolution dictate that rather than closing the incident, the incident should have a state of Resolved. This state gives the service desk a mechanism to verify that caller is satisfied with the resolution, and that the customer agrees with closing the incident.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Best Practice - ITIL KPI Reports</td>
<td>com.snc.bestpractice.itil_kpi</td>
<td>Provides a series of reports that track the Key Performance Indicators (KPI) of incident management and problem management.</td>
<td>Active</td>
<td>true</td>
<td>com.glide.metrics</td>
</tr>
<tr>
<td>Business Location</td>
<td>com.snc.business_location</td>
<td>This plugin supports a data model where the corporation does business with customers through physical channels such as stores and branches.</td>
<td>Active</td>
<td>true</td>
<td>• com.snc.service_organization • com.snc.cs_base_extension</td>
</tr>
<tr>
<td>Business Roles</td>
<td>com.snc.businessroles</td>
<td>Activates the Business Roles module. Combined with other licensed applications, provides business roles and hierarchy for employees with integration to Okta for access provisioning during onboarding.</td>
<td>Inactive</td>
<td>false</td>
<td>com.sn_content_delivery</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Business Rule V2</td>
<td>com.glide.business_rule_v2</td>
<td>Enhances business rules to support script-free conditions and behaviors.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Business Stakeholder</td>
<td>com.snc.business_stakeholder</td>
<td>Contains the Business Stakeholder role which authorizes the users to approve, view/read records across the organization and view reports. Note there is a fee associated with the Business Stakeholder role. Do not assign it to users without confirming your organization has the appropriate entitlement.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Cache build stats</td>
<td>com.glide.stats.cache_build</td>
<td>Cache build stats.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.stats</td>
</tr>
<tr>
<td>Card Operations (New in Quebec)</td>
<td>com.sn_bom_credit_card</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Case Assignment Workbench Demo</td>
<td>com.snc.case_assignment_workbench_demo</td>
<td>Provides demo data, such as sample cases and users, so that the Assignment Workbench product features can be demonstrated on a non-production instance. Not for use on customer production instances.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.customerservice, com.snc.assignment_workbench</td>
</tr>
<tr>
<td>Case Digests</td>
<td>com.sn_csm_case_digest</td>
<td>Enables users to send case status updates and root cause analysis to customers and key internal stakeholders.</td>
<td>Inactive</td>
<td>true</td>
<td>com.sn_customerservice, com.sn_csm_doc_template, com.snc.documentviewer, com.sn_publications</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>-------------------------------------------------------------------</td>
</tr>
<tr>
<td>Case Playbook for Complaints</td>
<td>com.sn_csm_complaint_case</td>
<td>Provides a complaint case type to capture the details for a customer complaint and a playbook that provides step-by-step guidance through the lifecycle of the complaint.</td>
<td>Active</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>Case Playbook for Onboarding</td>
<td>com.sn_csm_onboarding_case</td>
<td>Provides an onboarding case type to capture the details when onboarding customers for a product or service and a playbook that provides step-by-step guidance through the lifecycle of the onboarding process.</td>
<td>Active</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>Case Playbook for Product Support</td>
<td>com.sn_csm_product_support</td>
<td>Case Flow for Product Support guides customer service agents through the steps needed to resolve product issues.</td>
<td>Active</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>Catalog Designer Common</td>
<td>com.glide.ui.ng.cc</td>
<td>Catalog Designer Common.</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.ui.ng.dc • com.glideapp.workflow</td>
</tr>
<tr>
<td>Central Dispatch</td>
<td>com.snc.central_dispatch</td>
<td>Allows visually allocating tasks to agents for a logged in dispatcher.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.dhtmlx.scheduler</td>
</tr>
<tr>
<td>Centralized Connection and Credential</td>
<td>com.snc.core.automation.com</td>
<td>Centralized Connection and Credential components.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Certification Core</td>
<td>com.snc.certification_core</td>
<td>Core certification structures such as filters and templates. Certification Core is activated automatically when any of these applications are activated:  • Desired State Certification (active by default)  • Architecture Compliance  • Data Certification  • IT Governance Risk and Compliance</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.list_v2  • com.snc.version</td>
</tr>
<tr>
<td>Change Management - Approval Policy</td>
<td>sn_chg_pol_appr</td>
<td>Change Management feature that helps in generating and configuring approvals using the Change Approval policies.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Change Management - ATF Tests</td>
<td>com.snc.change_management</td>
<td>This plugin loads ATF tests for Change Management when the Change Management - State Model plugin is active. The demo data for this plugin is required to successfully execute these ATF tests.</td>
<td>Inactive</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>Change Management - CAB Workbench</td>
<td>com.snc.change_management</td>
<td>Change Management feature which allows CAB Managers to schedule, plan and manage CAB Meetings all on the NOW platform.</td>
<td>Active</td>
<td>true</td>
<td>• com.snc.change_management.cab.form_layout  • com.snc.app.calendar  • com.glide.service-portal  • com.snc.app_common.service_portal  • com.glide.editor.tinymce</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------</td>
<td>----</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
<td>---------------</td>
</tr>
</tbody>
</table>
| Change Management - Case Intelligence (New in Quebec) | com.snc.change_management.ml | Management feature that uses Predictive Intelligence to automatically identify cases that may have been caused by change. | Inactive | false | • com.snc.change_management.ml
| Change Management - Change Model Foundation Data (New in Quebec) | com.snc.change_management.chm | Change Models, including State transitions and supporting flows. | Active | false | • com.snc.change_management.change_model.foundation
| Change Management - Change Models (New in Quebec) | com.snc.change_management.chm | Change Models allow flexible configuration of state and transition models for Change Requests. | Active | false | • com.snc.itsm.state_transition_model
| Change Management - Change Models Landing (New in Quebec) | com.snc.change_management.chm | Change model landing user interface used to create Change Requests based on Change Models. | Active | false | com.snc.change_management.change_model.landing
| Change Management - Foundation Data (New in Quebec) | com.snc.change_management.foundation | Change Management foundation data, new states, priorities. | Active | true | com.snc.change_management
| Change Management - Change Related Incidents (Maintenance mode) | com.snc.change_management.icbc | Configuration for Change Related Incidents Classic UI | Active | false | com.snc.change_request
| Change Management - Change Schedule | com.snc.change_management.soc | Change Schedule. | Active | false | • com.snc.dhtmlx.gantt
| | | | | | • com.snc.change_request
| | | | | | • com.snc.change_management.soc.color_picker

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Management - Change Schedule foundation</td>
<td>com.snc.change_management</td>
<td>ChangeManagement - Change Schedule Foundation Data.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.change_management.soc</td>
</tr>
<tr>
<td>Change Management - Change Success Score New in Quebec.</td>
<td>com.snc.change_management</td>
<td>ChangeSuccess_score</td>
<td>Active</td>
<td>false</td>
<td>com.snc.change_management.soc</td>
</tr>
<tr>
<td>Change Management - Collision Detector</td>
<td>com.snc.change_management</td>
<td>Conflict Detection is a feature of the Change Management application which identifies potential scheduling conflicts based on the configuration items in scope for the change or user or group assigned to fulfill a change.</td>
<td>Active</td>
<td>true</td>
<td>com.snc.maintenance_schedules</td>
</tr>
<tr>
<td>Change Management - Color Picker</td>
<td>com.snc.change_management</td>
<td>ColorPicker</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>-------------------------------------------------</td>
</tr>
</tbody>
</table>
| Change Management - Core       | com.snc.change_management   | Core change management plugin which both Change Management State Model and Standard Change Catalog plugins depend on. This plugin updates the **Type** field on Change Request to have the values **Normal**, **Standard**, and **Emergency**. The Type value on existing Change Requests is updated:  
  • Routine  
    com.glide.context_help-> standard  
    (Standard)  
  • Comprehensive  
    -> normal  
    (Normal)  
  • Emergency  
    -> emergency  
    (Emergency)  
When creating a Change Request, an interceptor prompts you for the type of Change you want to create. | Active | true                      | • com.snc.change_request  
• com.snc.change_collision     |
| Change Management - Incident Intelligence | com.snc.change_management | Change Management feature that uses Predictive Intelligence to automatically identify incidents that may have been caused by change. | Active | false         | • com.snc.change_management.ml  
• com.snc.change_management.icbc |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
</table>
| Change Management - Mass Update CI | com.snc.change_management.mass_update_ci | Change Management feature which allows change requesters to propose and apply updates associated with a change request to one or more configuration items in scope for a change. | Inactive | false | • com.snc.change_management.state_model
• com.snc.bestpractice.bulkchange |
| Change Management - Predictive Intelligence Core (maintenance mode) | com.snc.change_management.ml | Core plugin containing the common components used by the Change Management Intelligence features. | Active | false | • com.snc.change_request
• com.glide.platform_ml |
| Change Management - Risk Assessment | com.snc.change_management.state_model | Change Management feature which allows risk assessment questionnaires to be created and required to drive the assessment of risk associated with a requested change. | Inactive | true | • com.snc.bestpractice.change_risk
• com.snc.assessment_core
• com.glide.assessment_designer |
| Change Management - Standard Change Catalog | com.snc.change_management.standard_change_catalog | Change Management feature which allows Standard change templates to be proposed, approved, and published in the ServiceNow Service Catalog. | Active | true | • com.snc.change_management
• com.glideapp.servicecatalog |
| Change Management - State Model | com.snc.change_management.state_model | This plugin provides the current Change Management state models for Standard, Normal and Emergency change types, originally released in the Geneva release. | Active | true | • com.snc.change_management
• com.snc.process_flow_formatter |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Management - Risk</td>
<td>com.snc.change_management</td>
<td>Change Management feature that augments existing risk assessment capabilities with Predictive Intelligence to predict change risk.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.change_management.ml</td>
</tr>
<tr>
<td>Intelligence (maintenance</td>
<td>com.snc.change_management</td>
<td>Change Management feature that uses Predictive Intelligence to identify change clusters that may be candidates for standard change templates.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.change_management.ml</td>
</tr>
<tr>
<td>only)</td>
<td>com.snc.change_management</td>
<td>Change Management Workflows</td>
<td>Active</td>
<td>true</td>
<td>com.glideapp.workflow</td>
</tr>
<tr>
<td>Change Request</td>
<td>com.snc.change_request</td>
<td>The base Change Request plugin which contains the core tables for Change Management, including the change request and change task tables.</td>
<td>Active</td>
<td>true</td>
<td>com.glideapp.report.itsm.change.overview</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Change Request Calendar</td>
<td>com.snc.change_request_calendar</td>
<td>This plugin activates the Change Conflict Calendar introduced in the Kingston release. It enables you to view a change request and its potential conflicts once a primary configuration item, planned start date, and planned end date have been provided within a Change request.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.app.calendar</td>
</tr>
<tr>
<td>Channel Proxy</td>
<td>com.glide.channelproxy</td>
<td>Contains the Business Stakeholder role which authorizes the users to approve, view/read records across the organization and view reports. Note there is a fee associated with the Business Stakeholder role. Do not assign it to users without confirming your organization has the appropriate entitlement.</td>
<td>inactive</td>
<td>false</td>
<td>com.glide.external.app</td>
</tr>
<tr>
<td>Checklist</td>
<td>com.glide.ui.checklist</td>
<td>Provides a simple way to track the progress of tasks without creating additional records, using checklists that can be added to any form.</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.ui.ng</td>
</tr>
<tr>
<td>C IDC Spoke</td>
<td>com.sn_cicd_spoke</td>
<td>Provides subflows and actions to call the Continuous Integration Continuous Delivery REST API endpoints included in the com.glide.continuous.delivery plugin.</td>
<td></td>
<td></td>
<td>• com.glide.rest.service</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Client Transaction Timings</td>
<td>com.glide.client_transaction</td>
<td>The Client Transaction plugin provides support to track client rendering times at the server, lining the values up with the server transaction times.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
</tbody>
</table>
| Cloud API                    | com.snc.cloud.api    | Cloud API Framework.                                                         | Inactive | false          | • com.snc.core.automation
• com.glide.ui.angular
• com.glide.ui.heisenberg
• com.snc.discovery.core                                                                 |
| Cloud Config Management      | com.snc.config.mgmt  | Config Management Framework.                                                 | Inactive | false          | • com.glide.rest
• com.snc.cloud.core                                                                 |
| Cloud Insights (Maintenance mode only) New in Quebec. | com.sn_clin | This plugin provides Azure provider specific insights                        | Active  | false          |                                                                              |
| Cloud Provisioning and Governance | com.snc.cloud.mgmt | Cloud Provisioning and Governance - Integration with AWS, Azure, VMware OOB and extensible to add support for new clouds. | Inactive | false          | • com.glide.service-portal
• com.snc.cloud.core
• com.snc.config.mgmt
• com.snc.runbook_automation                                                                 |
| Cloud Provisioning and Governance Core | com.snc.cloud.core | Cloud Provisioning and Governance Core - Discovery and Resource Blocks.     | Inactive | false          | • com.snc.discovery.core
• com.snc.cloud.api                                                                 |
| Cloud Spend Dashboard (Available in the ServiceNow Store) New in Quebec. | sn_sam_cld_spend | This plugin provides Insights into SaaS, IaaS and PaaS Spend and Savings    | Active  | false          | • com.snc.cloud.api
• com.snc.cmdb.scoped
• com.snc.discovery
• com.itom.jutils
• com.sn_itom_opt_licensing
• com.snc.clotho
• com.glide.hub.integration.runtime
• com.glide.hub.integrations.standard
• com.sn_sam_saas                                                                 |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMDB-ATF Tests</td>
<td>com.snc.cmdb.atf</td>
<td>Provides the CMDB Automated Test Framework (ATF) tests.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.cmdb</td>
</tr>
</tbody>
</table>
| CMDB Dashboard    | com.snc.cmdb.dashboard | Report overall CMDB and class level aggregated CI health.                  | Active | false          | • com.snc.cmdb
                              |                     |                                                              |        |                | • com.snc.pa
                              |                     |                                                              |        |                | • com.glideapp.canvas
| CMDB Group        | com.snc.cmdb.group  | Provides Configuration Item grouping capabilities.                          | Active | false          |                                        |
| CMDB Group Dashboard | com.snc.cmdb.group.dashboard | Report the health of CIs in CMDB Groups, on a dashboard.                    | Active | false          | • com.snc.cmdb
                              |                     |                                                              |        |                | • com.snc.pa
                              |                     |                                                              |        |                | • com.glideapp.canvas
<pre><code>                          |                     |                                                              |        |                | • com.snc.cmdb.group |
</code></pre>
<p>| CMDB Mainframe    | com.snc.cmdb.mainframe | One of the plugins included in the Extended CMDB plugin, used for mainframe configuration items. | Inactive | false          | com.snc.cmdb                          |
| CMDB Radio Category | com.snc.cmdb.radio.category | One of the plugins included in the Extended CMDB plugin, used for radio configuration items. | Inactive | false          | com.snc.cmdb                          |
| CMDB Search       | com.snc.cmdb_search | Query-like search on CMDB CIs and relationships. Converts a free-style query with configurable synonyms and stop words, into a properly formulated query on CMDB tables. | Active  | false          | com.snc.cmdb                          |
| CMDB Telecom Category | com.snc.cmdb.telecom.category | One of the plugins included in the Extended CMDB plugin, used for telecom configuration items. | Inactive | false          | com.snc.cmdb                          |</p>
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMDB Test Equipment</td>
<td>com.snc.cmdb.test.equipment</td>
<td>One of the plugins included in the Extended CMDB plugin, used for test equipment configuration items.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.cmdb</td>
</tr>
<tr>
<td>CMDB Workspace</td>
<td>com.cmdb-workspace</td>
<td>Enables CMDB capabilities in Agent Workspace.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.agent_workspace.itsm</td>
</tr>
</tbody>
</table>
| CMS User Interface - Service Management Core | com.snc.service_management.cmscontent | Management System items (blocks, pages, and menus) used to reference core IT self-service applications are packaged in this plugin. It is also the core foundation for all Service Management applications. | Inactive  | false          | • com.glide.cms  
• com.glide.cms.extensions  
• com.glide.db_images |
| Coaching                                 | com.sn_coaching                | The Coaching module facilitates the coaching of employees on their work through the use of coaching opportunities (critical moments in a process) that can be conditionally configured. | Active    | true           | • com.snc.planned_task_v2  
• com.snc.skills_management  
• com.snc.organization_management |
<p>| Code Search                              | com.glide.code-search          | A configurable Code Search API.                                                                                                               | Active    | false          |                                                                                             |
| Collaboration                            | com.glide.collaboration        | Retired. Replaced by the Connect plugin.                                                                                                       | Inactive  | false          | com.glide.connect                                                                            |</p>
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collaboration Services</td>
<td>sn_tcm_collab_hook</td>
<td>Provides the ability to communicate over Slack.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.hub.integrations and com.sn.slack.ahv2</td>
</tr>
<tr>
<td>Note:</td>
<td></td>
<td><strong>Starting with the Paris release, the Collaboration Services for Task Communications Management plugin is renamed as Collaboration Services.</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collision APIs</td>
<td>com.glide.collision_detector</td>
<td>APIs for predicting the behavior of the upgrade engine with regard to customizations.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Column Statistics</td>
<td>com.glide.column_statistics</td>
<td>Column statistics used to suggest database indexes.</td>
<td>Active</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>Common ITSM Service Portal Application Components</td>
<td>com.snc.app_common.service</td>
<td><strong>Application Components for Service Portal.</strong></td>
<td>Active</td>
<td>false</td>
<td>com.glide.service-portal</td>
</tr>
</tbody>
</table>
| Communities                   | com.sn_communities             | Communities enable customers to interact with each other and share knowledge. There is no structured way to disseminate knowledge or capture knowledge from communities and make it a part of customer service and customer success. | Inactive | false          | • com.glide.service-portal  
• com.snc.activity_subscriptions  
• com.snc.gamification  
• com.snc.csm_unified_theme  
• com.snc.assignment_workbench  
• com.glide.processor.ics |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
</table>
| Communities Demo Data | com.sn_communities_demo | Loads demo data for the community application. | Inactive | false | • com.sn_communities
• com.snc.csm_unified_theme.demo |
<p>| Company extension | com.glide.company | Adds currency columns to the Company [core_company] table. | Active | false | com.glide.currency |
| Configuration Compliance (Available in the ServiceNow Store) | snc_vulc | Exposes your high-impact configuration-related security vulnerabilities, and orchestrates their remediation across frequently isolated information security, IT operations, and business process areas. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details. | Inactive | true | com.snc.security_support.common |
| Configuration Compliance Dependencies | snc_vulc_dep | System dependencies required by Configuration Compliance. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details. | | false | |
| Configuration Management (CMDB Enterprise Edition) | com.snc.cmdb.enterprise | A collection of modules for specialized configuration items, such as radio hardware, test equipment, and voice system hardware. | Active | false | com.snc.cmdb |</p>
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Management (CMDB)</td>
<td>com.snc.cmdb</td>
<td>Provides core functionality for the configuration management database, including enterprise hardware and configuration item relationships.</td>
<td>Active</td>
<td>true</td>
<td>• com.glide.custom_web_service</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.sn_cmdb_content</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.db.rotation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.ui.list_v3_components</td>
</tr>
<tr>
<td>Configuration Management For Scoped Apps (CMDB)</td>
<td>com.snc.cmdb.scoped</td>
<td>Enables scoped apps access to Identification Engine APIs.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.cmdb.enterprise</td>
</tr>
<tr>
<td>Connect</td>
<td>com.glide.connect</td>
<td>Provides a real-time messaging platform that connects you to your coworkers, bypassing email and static documents.</td>
<td>Active</td>
<td>false</td>
<td>• com.glideapp.live_feed</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glideapp.live_common</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.ui.ng</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.ui.angularui</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.ui.ng.amb</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.notification.push</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.db_audio</td>
</tr>
<tr>
<td>Connect Interaction UI</td>
<td>com.connect-interaction-ui</td>
<td>User interface components to adapt Connect Support to use the interaction table as a source of truth.</td>
<td>inactive</td>
<td>false</td>
<td>• com.glide.interaction</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.graphql</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.connect.support</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.connect.ui_components</td>
</tr>
<tr>
<td>Connect Scriptable APIs</td>
<td>com.glide.connect.scriptable</td>
<td>Scriptable APIs for Connect.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Connect Service Portal Widgets</td>
<td>com.glide.connect.sp_widgets</td>
<td>Connect Service Portal Widgets</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.service-portal</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.connect</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.connect.ui_components</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Connect Spoke for Flow Designer</td>
<td>com.glide.connect_v3plus.core.ah</td>
<td>The Connect Spoke for the Flow Designer provides actions that a process analyst can use when designing flows. The actions allow them to automate the creation of conversations, to add users to a conversation, and to send messages to a conversation. These actions work with Connect API version 3 and later.</td>
<td>Active</td>
<td></td>
<td>com.glide.connect.scriptable</td>
</tr>
<tr>
<td>Connect Support</td>
<td>com.glide.connect.support</td>
<td>Builds on the Connect messaging platform and enables support agents to provide real-time assistance to end users, using queues.</td>
<td>Inactive</td>
<td></td>
<td>com.glide.connect</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.connect.support</td>
</tr>
<tr>
<td>Connect Support Manager's Dashboard</td>
<td>com.glide.connect.managers</td>
<td>Provides a homepage and all the configuration records required to analyze Connect Support in reporting.</td>
<td>Inactive</td>
<td></td>
<td>com.glideapp.report</td>
</tr>
</tbody>
</table>
| Connect Support Routing                     | com.glide.connect.support.routing       | Plugin to enable processor for Routing Connect Support request to appropriate Chat Queue. | Inactive|               | • com.snc.matching_rule  
|                                              |                                         |                                                                               |       |               | • com.glide.connect.support                      |
| Consumer Service Portal                      | com.glide.service-portal.consumer-portal | Enables the Consumer Service Portal, a web-based portal based on the Service Portal application that your company can use to provide information and support to consumers. | Inactive|               | • com.glide.service-portal.customer-service-base  
<p>|                                              |                                         |                                                                               |       |               | • com.glide.connect.anonymous_support            |</p>
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Analytics</td>
<td>com.sn_content_analytics</td>
<td>Content Analytics</td>
<td>Active</td>
<td>false</td>
<td>com.glide.scope.access.restricted_caller</td>
</tr>
<tr>
<td>Content Automation</td>
<td>com.sn_content_automation</td>
<td>Content automation functionality.</td>
<td>inactive</td>
<td>true</td>
<td>• com.sn_content_delivery</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.scope.access.restricted_caller</td>
</tr>
<tr>
<td>Content Delivery</td>
<td>com.sn_content_delivery</td>
<td>Content Delivery</td>
<td>inactive</td>
<td>true</td>
<td>• com.glide.db_images</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.scope.access.restricted_caller</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.service-portal</td>
</tr>
<tr>
<td>Content Management</td>
<td>com.glide.cms</td>
<td>Allows administrators to create custom, branded, web user interfaces on top of an existing ServiceNow instance. You must request the Content Management System (CMS) application from ServiceNow personnel. Instead of activating CMS, use Service Portal for new development. Service Portal is an alternative to CMS with a refined user experience, and is active by default in the base system. See Service Portal and Content Management and Service Portal.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.glideapp.home</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.text_search</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.db_images</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Content Management Extended Types</td>
<td>com.glide.cms.types</td>
<td>An extension to Content Management that adds iFrames and Flash frames. You must request the Content Management System (CMS) application from ServiceNow personnel. Instead of activating CMS, use Service Portal for new development. Service Portal is an alternative to CMS with a refined user experience, and is active by default in the base system. See Service Portal and Content Management and Service Portal.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.cms.type.flash, com.glide.cms.type.iframe</td>
</tr>
<tr>
<td>Context-Sensitive Help</td>
<td>com.glide.context_help</td>
<td>Provides a context-sensitive help system, providing links to specific help pages. These help pages can be linked to the list or form view of any table, or to the form view of a specific record in a table.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Context-Sensitive Help Rest API</td>
<td>com.glide.context_help.rest_api</td>
<td>REST API for the context-sensitive help system</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.context_help</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.scripted_rest_services</td>
</tr>
<tr>
<td>Contextual Search</td>
<td>com.snc.contextual_search</td>
<td>Display related articles or service catalog items within a form or record producer.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.application.json_service</td>
</tr>
<tr>
<td>Contextual Search - Internal</td>
<td>com.snc.contextual_search.internal</td>
<td>Internal plugin component for Contextual Search.</td>
<td>Active</td>
<td>false</td>
<td>• com.snc.contextual_search</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.app_common.service_portal</td>
</tr>
<tr>
<td>Contextual Search - Service Portal</td>
<td>com.snc.contextual_search.service-portal</td>
<td>Service Portal components for Contextual Search.</td>
<td>Active</td>
<td>false</td>
<td>• com.snc.contextual_search</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.app_common.service_portal</td>
</tr>
<tr>
<td>Contextual Security: Role Management</td>
<td>com.glide.role_management</td>
<td>Provides the flexibility and power to protect information by controlling read/write/create/delete authorization.</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.db_view</td>
</tr>
<tr>
<td>Contextual Security: Role Management V2</td>
<td>com.glide.role_management</td>
<td>Prevents duplicate entries in sys_user_has_role for inherited roles, based on the value of the inh_count column.</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.role_management.inh_count</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.scripted_rest_services</td>
</tr>
<tr>
<td>Contextual Security: Role Management V2 REST API</td>
<td>com.glide.role_management</td>
<td>Prevents duplicate entries in sys_user_has_role for inherited roles, based on the value of the inh_count column.</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.role_management.inh_count</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.scripted_rest_services</td>
</tr>
<tr>
<td>Continual Improvement Management (CIM)</td>
<td>com.sn_cim</td>
<td>Core plugin for Continual Improvement Management (CIM)</td>
<td>Active</td>
<td>true</td>
<td>• com.snc.organization_management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.planned_task_v2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.pa</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.pa.spotlight</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.sn_coaching</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.sn_cim_atf</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Continual Improvement Management Automated Tests</td>
<td>com.sn_cim_atf</td>
<td>ATF plugin for Continual Improvement Management (CIM)</td>
<td>Active</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>Contract Management</td>
<td>com.snc.contract_management</td>
<td>Provides the ability to manage all types of contracts.</td>
<td>Active</td>
<td>true</td>
<td>com.snc.asset_management</td>
</tr>
<tr>
<td>Contract Management - Form Layouts and Behavior</td>
<td>com.snc.contract_management</td>
<td>Provides the ability to customize the Contract Management form layout.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Conversation Branding Settings</td>
<td>com.glide.cs.branding</td>
<td>Conversation Branding Settings for web chat client.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Conversation General Settings</td>
<td>com.glide.cs.settings</td>
<td>Conversation General Settings for Virtual Agent.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Conversational Interfaces Guided Setup (New in Quebec)</td>
<td>com.glide.ci_guided_setup</td>
<td>Provides customers with a visual guidance to configure Conversational Interfaces.</td>
<td>Active</td>
<td>false</td>
<td>• com.snc.guided_setup • com.glide.guided_setup_config</td>
</tr>
<tr>
<td>Conversational Messaging</td>
<td>com.glide.messaging.awa</td>
<td>Conversational Messaging</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conversational SMS Integration with Twilio Maintenance mode</td>
<td>com.sn.va.sms.twilio</td>
<td>Integration to SMS for Advanced Work Assignment</td>
<td>Active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CORS support for REST API</td>
<td>com.glide.rest.cors</td>
<td>CORS support for REST API</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Cost Management</td>
<td>com.snc.cost_management</td>
<td>Tracks operating costs for configuration items and task-related activities, allocates the costs to business consumers, and compares actual allocations to planned budgets.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.expense_line</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>Cross-scope Access</td>
<td>com.glide.scope.access</td>
<td></td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Cross-scope App Privilege Enforcement</td>
<td>com.glide.scope.privilege</td>
<td>System for capturing and enforcing cross-scope privileges used by Scoped Apps</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>CSM Extension for Proxy Contacts</td>
<td>com.snc.csm_proxy_contacts</td>
<td>Enables users who are internal to an organization to be the proxy case contact on behalf of customers.</td>
<td>Inactive</td>
<td>true</td>
<td>com.sn_customerservice</td>
</tr>
<tr>
<td>CSS Theme support</td>
<td>com.glide.ui.themes</td>
<td>Provides support for CSS customizations to the user interface.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.ui.themes.core</td>
</tr>
<tr>
<td>CSS Theme support - UI 14</td>
<td>com.glide.ui.themes.doctype</td>
<td>Provides UI15 themes.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.ui.themes.core</td>
</tr>
<tr>
<td>CTI Demo Data for HRSD</td>
<td>com.sn_hr_cti_demo</td>
<td>Provides CTI Softphone application demo data for HRSD.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.snc.cti</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.matching_rule</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.sn_openframe</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.notify</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.notify.twilio_direct</td>
</tr>
<tr>
<td>CTI Softphone</td>
<td>com.snc.cti</td>
<td>Enables Twilio integration using Notify and OpenFrame to provide softphone functions and call center capabilities. These include make, receive phone calls, transfer, hold and mute. Applications like Customer Service and Incident Management provide demo workflows for CTI.</td>
<td>Active</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>Credit Assessment</td>
<td>com.sn_bom_credit_asmt</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(New in Quebec)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| CSM and FSM Configurable Workspace Foundation (New in Quebec) | com.snc.uib.cwf_workspace        | Supports refactored version of customer workflow agent workspace.            | Inactive| false          | • com.snc.app_shell_aw  
  • com.snc.uib.base_agent_workspace  
  • com.snc.uib.cwf_workspace.integrations |
| CSM Configurable Workspace (New in Quebec)  | com.snc.uib.csm_agent_workspace  | Supports refactored version of customer workflow customer service management agent workspace. | Active  | true           | • com.snc.uib.cwf_workspace  
  • com.glideapp.servicecatalog.uxfworkspace  
  • com.snc.uib.lookup_verify  
  • com.devsnc_sn_response_templates |
<p>| CSM Configurable Workspace Lookup and Verify (New in Quebec)  | com.snc.uib.lookup_verify        | Installs Lookup and Verify artifacts for the CSM Configurable Workspace which includes pages, macroponents, data brokers etc. and can be shared in different applications. | Inactive| true           | com.snc.sn_csm_lookup_verify                                                |
| CSM Configurable Workspace Special Handling Notes (New in Quebec)  | com.snc.uib.special_handling     | <strong>Installs</strong> Special Handling Notes artifacts for the CSM Configurable Workspace which includes pages, macroponents, data brokers etc. and can be shared in different applications. | Inactive| false          |                                                                             |
| CSM Contributor User (New in Quebec)       | com.snc.csm_contributor_user     | Allows you to enable contributors to report and collaborate on cases created for customers, service organizations, or themselves. | Active  | true           | com.snc.cs_base_extension                                                   |</p>
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Currency support for the service catalog</td>
<td>com.glideapp.servicecatalog.currency</td>
<td>Enables service catalog to support fully localized currencies for item prices and options.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.currency</td>
</tr>
<tr>
<td>Custom URL</td>
<td>com.snc.customurl</td>
<td>Activate this plugin to set up custom URL on the instance.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.customurl.internal</td>
</tr>
<tr>
<td>Custom URL - Internal</td>
<td>com.snc.customurl.internal</td>
<td>An internal plugin component to Scripted CustomURL APIs.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Customer Communities</td>
<td>com.sn_customer_communities</td>
<td>Enables you to connect, engage, and collaborate with your employees, customers, partners, and prospects. It is only available for customers who are licensed for Customer Services Management.</td>
<td>Inactive</td>
<td>false</td>
<td>com.sn_external_user_register • com.sn_communities</td>
</tr>
<tr>
<td>Customer Project Management</td>
<td>com.snc.csm_ppm</td>
<td>Provides the ability to create and manage projects for a customer account and gives end users visibility into their projects via the portal. This plugin requires the Customer Service plugin and the Project Portfolio Suite with Financials plugin.</td>
<td>Inactive</td>
<td>true</td>
<td>com.sn_customerservice • com.snc.financial_planning_pmo</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
</table>
| Customer Service       | com.sn_customerservice    | Enables you to provide service and support for your external customers using several communication channels, such as email, web, and telephone. A case is created to track the issue reported or service requested, and assigned to groups or agents. Customer service agents in your organization work on the cases and resolve issues. | Inactive| false          | com.snc.asset_management  
|                        |                           |                                                                               |         |                | com.snc.state_flows      
|                        |                           |                                                                               |         |                | com.glide.connect.support 
|                        |                           |                                                                               |         |                | com.glide.connect.support.routing 
|                        |                           |                                                                               |         |                | com.snc.assignment_workbench 
|                        |                           |                                                                               |         |                | com.snc.cs_base          
|                        |                           |                                                                               |         |                | com.snc.skills_management   
|                        |                           |                                                                               |         |                | com.snc.assessment_core 
|                        |                           |                                                                               |         |                | com.snc.process_flow_formatter   
|                        |                           |                                                                               |         |                | com.snc.task_relations      
|                        |                           |                                                                               |         |                | com.snc.task_activity       
|                        |                           |                                                                               |         |                | com.snc.matching_rule      
|                        |                           |                                                                               |         |                | com.snc.resolutionshaper 
|                        |                           |                                                                               |         |                | com.snc.openframe        
|                        |                           |                                                                               |         |                | com.snc.shn             
|                        |                           |                                                                               |         |                | com.snc.contextual_search.dynamic_filters      
|                        |                           |                                                                               |         |                | com.snc.cs_social       
| Customer Service Base  | com.snc.cs_base_extension | This plugin provides granular access control through relationships, user profile attributes and roles. | Active  | false          | com.sn_customerservice   
| Extension Entities     |                           |                                                                               |         |                |                                                                           
| Customer Service Case  | com.snc.csm_case_types    | Enables customers to manage complex case processes by defining new case types. A case type represents an individual business process and is a collection of diverse inputs and tasks that an agent performs to resolve customer requests. | Inactive| true           | com.sn_customerservice    
| Types                  |                           |                                                                               |         |                |                                                                           
| Customer Service CTI    | com.snc.customerservice_cti| Provides demo data for the CTI Softphone application.                        | Inactive| false          | com.sn_customerservice  
| Demo Data              |                           |                                                                               |         |                | com.snc.cti                

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Service Household</td>
<td>com.snc.household</td>
<td>Enables managing customer service for consumers belonging to the same household. Provides the ability to define the members of a household and relationships between them.</td>
<td>Active</td>
<td>true</td>
<td>com.snc.cs_base_extension</td>
</tr>
<tr>
<td>Customer Service Install Base Management</td>
<td>com.snc.install_base</td>
<td>Enables customers to capture the current state of a customer's install base and establish the relationship to any downstream entities that might impact their functioning.</td>
<td>Inactive</td>
<td>false</td>
<td>com.sn_customerservice</td>
</tr>
</tbody>
</table>
| Customer Service Management Demo Data | com.snc.customerservice.demo | Provides demo data for the Customer Service Management application. | Inactive| false          | • com.sn_customerservice
• com.glide.service-portal.consumer-portal
• com.glide.service-portal.customer-portal
• com.snc.case_assignment_workbench.demo
• com.snc.work_management.demo
• com.snc.planned_maintenance
• com.snc.kb_product_entitlements
• com.snc.publications_demo
• com.snc.shn_demo
• com.snc.csm.order
• com.snc.csm_fsm_integration |
<p>| Customer Service Management for Orders | com.snc.csm.order  | Extends the Customer Service Management application to support order-related issues by integrating with order management systems to create and resolve customer requests. | Inactive| true           | com.sn_customerservice                                                     |</p>
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Service Mobile</td>
<td>com.sn_csm_mobile</td>
<td>Enables the mobile user interface for Customer Service Management.</td>
<td>Inactive</td>
<td>false</td>
<td>com.sn_customerservice</td>
</tr>
<tr>
<td>Customer Service NLU Model for Virtual Agent Conversations</td>
<td>com.sn_csm.nlu</td>
<td>Enables CSM Virtual Agent conversations.</td>
<td>Active</td>
<td>false</td>
<td>• com.sn_customerservice&lt;br&gt;• com.glide.cs.chatbot&lt;br&gt;• com.glide.cs.sn-va-web-client-app</td>
</tr>
<tr>
<td>Customer Service Portal</td>
<td>com.glide.service-portal.customer-portal</td>
<td>Enables the Customer Service Portal, a web-based portal based on the Service Portal application that your company can use to provide information and support to customers.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.service-portal.customer-service-base</td>
</tr>
<tr>
<td>Customer Service Social Integration</td>
<td>com.sn_cs_social</td>
<td>Customer Service Social integration, currently adds appropriate data schema changes needed for social integration scenarios.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Customer Service Spoke</td>
<td>com.snc.customer_service.spoke</td>
<td>Enables Flow Designer users to automate the creation of customer service cases and updates to existing cases.</td>
<td>Inactive</td>
<td>false</td>
<td>Flow Designer - Installer (com.glide.hub)</td>
</tr>
<tr>
<td>Customer Service Virtual Agent Conversations</td>
<td>com.sn_csm.virtualagent</td>
<td>CSM Virtual Agent Conversations</td>
<td>Active</td>
<td>false</td>
<td>• com.sn_customerservice&lt;br&gt;• com.glide.cs.chatbot&lt;br&gt;• com.glide.cs.sn-va-web-client-app</td>
</tr>
<tr>
<td>Customer Service with Field Service Management</td>
<td>com.snc.csm_fsm_integration</td>
<td>Enables Account, Contact, Partner, Partner Contact, Consumer information from Customer Service to Field Service Management.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.snc.work_management&lt;br&gt;• com.sn_customerservice&lt;br&gt;• com.glide.service-portal.customer-portal</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Customer Service Install Base Management</td>
<td>com.snc.install_base</td>
<td>Enables customers to capture the current state of their install base and establish the relationship to any downstream entities that might impact their functioning.</td>
<td>Inactive</td>
<td>false</td>
<td>com.sn_customerservice</td>
</tr>
<tr>
<td>Data Archiving</td>
<td>com.glide.auxdb</td>
<td>Provides the ability to move a subset of data from large tables into the data archive. Typical candidates include historical ITIL documents such as incidents which were closed last year, but the functionality supports archiving of non ITIL documents as well.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.db.replicate</td>
</tr>
<tr>
<td>Data Classification</td>
<td>com.glide.data_classification</td>
<td></td>
<td>Active</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>---------------------</td>
<td>-------------</td>
<td>---------</td>
<td>----------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Data Certification</td>
<td>com.snc.certification_v2</td>
<td>Enables field-level certification of data, either scheduled or on-demand.</td>
<td>Inactive</td>
<td>true</td>
<td>• com.glide.list_v2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.certification_core</td>
</tr>
<tr>
<td>Data Lookup and Record Matching Support</td>
<td>com.glide.data_lookup</td>
<td>Allows administrators to define rules that automatically set one or more field values when certain conditions are met. This plugin completely replaces Priority Lookup. Any custom logic defined in the CalculatePriority business rule must be manually translated into the new priority data lookup definition.</td>
<td>Active</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>Data Lookup and Record Matching Support for Service Catalog</td>
<td>com.glide.data_lookup.catalog</td>
<td>Allows administrators to perform data lookups for variables on service catalog item screens, on requested items, and on catalog tasks as a user fills out the values contained in variables.</td>
<td>Active</td>
<td>false</td>
<td>• com.glideapp.servicecatalog.platform</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.data_lookup</td>
</tr>
<tr>
<td>Data Policy 2</td>
<td>com.glide.data_policy2</td>
<td>Defines mandatory or read-only requirements for table fields.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Data Structures</td>
<td>com.snc.datastructure</td>
<td>Provides element types: DataStructure and DataObject for flyweight data that can be stored internally as JSON and utilized via the DataStructure API.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Database Column Offrow Migration</td>
<td>com.glide.db.offrow_migration</td>
<td>UI/Script elements to allow for compatible columns to be moved offrow.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>---------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>Database Rotation</td>
<td>com.snc.db.rotation</td>
<td>Provides the ability to break large tables into smaller, more manageable tables; these smaller tables contain a specified period of data and the table with oldest data is purged on an ongoing basis.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Database Rotation with Default Tables</td>
<td>com.snc.db.rotation_default_tables</td>
<td>Adds database rotation functionality to default tables.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.db.rotation</td>
</tr>
<tr>
<td>Database Storage for Audio Files</td>
<td>com.glide.db_audio</td>
<td>Allows audio files to be uploaded and stored in the database, and referenced in HTML.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Database Storage for Images</td>
<td>com.glide.db_images</td>
<td>Allows images to be uploaded and stored in the database, and referenced in HTML.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Database Storage for Video Files</td>
<td>com.glide.db_video</td>
<td>Allows video files to be uploaded and stored in the database, and referenced in HTML.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Database Views</td>
<td>com.glide.db_view</td>
<td>Allows you to define table joins for reporting purposes.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>DataTables 1.1.0 Components</td>
<td>com.glide.ui.ng.datatables</td>
<td>DataTables 1.1.0 Components</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Default Financial Management Cost Model</td>
<td>com.snc.financial_management_model</td>
<td>Provides a preconfigured Cost Model and artifacts to enable Financial Analysts to assemble spending data and generate reports. Activation of this plugin on production instances may have licensing implications. Contact your ServiceNow account team for details.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.financial_management</td>
</tr>
<tr>
<td>Delegated Dev User Administration</td>
<td>com.sn_dd_user_admin</td>
<td>Delegated Dev User Administration.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Delegated Development</td>
<td>com.glide.delegated_development</td>
<td>Support for controlled development by users who do not have full administrative rights.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Delegated Request Experience (Maintenance mode)</td>
<td>com.glideapp.servicecatalog.request_management.delegated_request_experience</td>
<td>Enables delegated requests for catalog items and activates the Requested For variable type and the Requested For field in Requested Item</td>
<td>Active</td>
<td>false</td>
<td>com.glideapp.servicecatalog.platform</td>
</tr>
<tr>
<td>Delete Recovery</td>
<td>com.glide.delete_recovery</td>
<td>Provides the ability to recover individual deleted items including all related cascaded deleted items.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Delete Recovery: Partial Undelete Support</td>
<td>com.glide.delete_recovery.partial_undelete</td>
<td>Delete Recovery plugin to support partially undeleting records from a transaction.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.delete_recovery</td>
</tr>
<tr>
<td>Demand Core</td>
<td>com.snc.demand_core</td>
<td>Demand Core Plugin aids in planning, organizing and managing Demands with basic features.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
<td>---------------------------------------------------</td>
</tr>
</tbody>
</table>
| Demand Management          | com.snc.demand_management   | Aids with capturing the demand and provides tools to screen, assess, and prioritize it. Only upgrade is allowed for this plugin. Activation should be done through PPM Standard plugin. | Inactive| true           | • com.snc.process_flow_formatter  
• com.snc.assessment_core  
• com.snc.timeline_visualization  
• com.snc.bubblechart_workbench |
| Depreciation               | com.snc.depreciation        | Core depreciation capabilities.                                              | Active  | false          |                                                   |
| Designer Common            | com.glide.ui.ng.dc         | Provides common components required by designers such as the form designer and the quiz designer. | Active  | false          | • com.glide.ui.tablet.theme  
• com.glide.ui.ng  
• com.glide.ui.themes.doctype |
<p>| Desired State Certification| com.snc.certification_desired | Evaluates records to see if they match a desired state, scheduled or on-demand. | Active  | true           | com.snc.certification_core                        |
| DevOps (Available in the ServiceNow Store) | sn_devops                  | Provides data insights, accelerates change, and increases visibility into your DevOps environment. |         |                |                                                   |
| DevOps Insights (Available in the ServiceNow Store) | sn_devops_insights      | Shows the results of your overall DevOps process in a data-driven dashboard. |         |                |                                                   |
| DHTMLX Gantt Library       | com.snc.dhtmlx.gantt        | DHTMLX Gantt library.                                                        | Inactive| false          |                                                   |
| DHTMLX Scheduler Library   | com.snc.dhtmlx.scheduler    | DHTMLX Scheduler library.                                                    | Active  | false          |                                                   |
| Diagnostic Monitoring      | com.glide.monitor.diagnostics | Provides advanced diagnostic monitoring of each node in a ServiceNow instance. | Active  | false          |                                                   |</p>
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dictionary overrides</td>
<td>com.glideictionary_override</td>
<td>Allows specific Dictionary values to be overridden for extended table elements. For example, this plugin allows the default value for the Assigned To field in the Incident table to be different than the default value specified for the Assigned To field in the Task table.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Discovery and Service Mapping Patterns</td>
<td>com.sn_itom_pattern</td>
<td>This plugin deploys additional Discovery and Service Mapping Patterns.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distribution Download Proxy</td>
<td>com.glide.dist_download_pro</td>
<td>Proxy for downloading a distribution. This plugin is activated automatically when the MID Server is activated, to handle the REST requests for file downloads that a MID Server sends to the instance.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Document Service (New in Quebec)</td>
<td>com.sn_bom_document</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------</td>
<td>----</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Domain Support - Domain Extensions Installer</td>
<td>com.glide.domain.msp_extensions.Installer</td>
<td>Enables domain separation for Cloud Provisioning and Governance. Instances activating Domain separation should use this plugin. In addition to functionality in the Domain Support plugin, this plugin installs Domain Support - Domain Extensions that include further domain separation enhancements for all domain customers including Managed Service Providers. If the Domain Support plugin is already active, content in the Domain Support - Domain Extensions plugin will not be installed to the instance.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Dynamic Scheduling</td>
<td>com.snc.dynamic_scheduling</td>
<td>Dynamic scheduling for Service Management Applications with support for bulk task recommendations and interval based auto assignment.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.snc.matching_rule • com.snc.service_management.core</td>
</tr>
<tr>
<td>Dynamic Translation</td>
<td>com.glide.dynamic_translation</td>
<td>Adds ability to translate the given text from source language to target language using external machine translation providers.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.hub.integrations</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Dynamic Translation Spoke (New in Quebec)</td>
<td>com.glide.dynamic_translation</td>
<td>Provides actions that enable the ability to translate text(s) from one language to other language(s) and to detect the language of given text.</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.hub</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.hub.integration.runtime</td>
</tr>
<tr>
<td>E164 Compliant Phone Number</td>
<td>com.glide.phone_number</td>
<td>Ensures that all necessary information for a phone number is included and properly formatted to successfully route an international call over a territory's public telephone network.</td>
<td>Active</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>Email - OAUTH support for IMAP and SMTP</td>
<td>com.glide.email.oauth</td>
<td>Support for XOAUTH and XOAUTH2 email authentication.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.glide.email_accounts</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.platform.security.oauth</td>
</tr>
<tr>
<td>Email Access Restriction</td>
<td>com.glide.email_access_restriction</td>
<td>Allows email table ACL conditional overrides</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Email Accounts</td>
<td>com.glide.email_accounts</td>
<td>Enables you to define email accounts and settings in individual records.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Email Address Filter</td>
<td>com.glide.email_address_filter</td>
<td>APIs and data structures for email address filtering</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>Email Automatic User Creation</td>
<td>com.glide.email_createuser</td>
<td>Sets glide.email.create_user so that when automatic user creation is enabled, the UserID of newly-created users matches the user's email address. Also widens sys_user.user_name column to 100 bytes to accommodate longer UserIDs based on email addresses.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.email_address_filter</td>
</tr>
<tr>
<td>Email Client</td>
<td>com.glide.email_client</td>
<td>Enables you to send email directly from any record</td>
<td>Active</td>
<td>false</td>
<td>com.glide.email_address_filter</td>
</tr>
<tr>
<td>Email Client Template</td>
<td>com.glide.email_client_template</td>
<td>Template defines default content for the Email Client.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Email Digest</td>
<td>com.glide.email_digest</td>
<td>Email Digest</td>
<td>Active</td>
<td>false</td>
<td>• Subscription Based Notifications</td>
</tr>
<tr>
<td>Email Filters</td>
<td>com.glide.email_filter</td>
<td>Filters emails into different mailboxes or junk, depending on headers and subject. Ignores any email that contains a VCAL invitation.</td>
<td>Inactive</td>
<td>false</td>
<td>• Outbound Email Notifications</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.notification.preference.service</td>
</tr>
<tr>
<td>Email Notification Preview Plugin</td>
<td>com.glide.email_notification_preview</td>
<td>Allows you to easily preview a ServiceNow email notification without sending the notification. This allows you to preview notifications at design time.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------</td>
<td>----</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Email Notification Script for Contextual Search Results</td>
<td>com.snc.adv_cxs_results_email_script</td>
<td>Provides script for embedding contextual search results based on Predictive Intelligence additional resources and search resources in email notifications.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
</tbody>
</table>
| Email Retention | com.glide.email_retention | Provides retention policy for email. | Active | false | • com.glide.mailbox  
• com.glide.auxdb |
| Email Service | com.glide.email.service | Defines javascript and REST API for sending email. | Active | false | com.glide.mailbox |
| Email Unsubscribe | com.glide.email_unsubscribe | Adds the ability to include an unsubscribe link in notifications. | Active | false | • com.glide.email_ordered_processing  
• com.glide.notification.subscription |
<p>| Email/SMS Separation | com.glide.email_sms_separation | Separation of the sending of SMS and email by adding a column to the email table. Prevents SMS messages from slowing down email message sending and vice versa. Activation of this plugin will cause email to stop sending during activation. On systems with large email tables this can take hours, and is not recommended. | Active | false | com.glide.notification |
| Embedded Help | com.glide.embedded_help | Provides targeted help content to a user in a UI page. Administrators can create customized embedded help to assist users with specific business processes within an organization. | Active | false | com.glide.ui.hopscotch |</p>
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedded Help for ServiceNow Flow Designer (New in Quebec)</td>
<td>com.glide.hub.flow_designer</td>
<td>Embedded Help for the embedded help panel in Flow Designer. In Quebec, there is a help panel to help users easily access documentation on Flow Designer without having to navigate to the documentation site.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Employee Document Management</td>
<td>com.sn_employee_document_management</td>
<td>Employee Document Management helps manage large numbers of employee documents efficiently. Provides storage space and a filing system that allows you to easily retrieve documents, as well as define who can view sensitive documents, and when to purge documents.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.documentviewer com.glide.scope.access.restricted_caller</td>
</tr>
<tr>
<td>Employee Service Center</td>
<td>com.sn_hr_service_portal</td>
<td>Activates a portal framework that allows administrators to build a mobile-friendly self service experience for users.</td>
<td>Active</td>
<td>true</td>
<td>com.glide.connect.support com.glide.connect.sp_widgets com.sn_content_delivery com.sn_content_automation com.glide.va.sp_widgets com.glideapp.user_criteria.scoped.api</td>
</tr>
</tbody>
</table>

**Important:**
To use Employee Document Management, the Human Resources Scoped App: Core plugin must be licensed and activated.
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypted Workflow Scratchpad</td>
<td>com.snc.encrypted.scratchpad</td>
<td>Encrypted Scratchpad support on the Workflow Context and Workflow Executing Activities.</td>
<td>Active</td>
<td>false</td>
<td>- com.glideapp.workflow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- com.glide.encryption</td>
</tr>
<tr>
<td>Encryption Core</td>
<td>com.glide.encryption.core</td>
<td>Common scripts and logic between Edge Encryption and Encryption Support.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Encryption Support</td>
<td>com.glide.encryption</td>
<td>Allows text fields and attached files to be encrypted.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.encryption.core</td>
</tr>
<tr>
<td>Encryption Support - Single Context Task Encryption Demo</td>
<td>com.snc.task_encryption.demo</td>
<td>Demo showing how encrypted form fields can be assigned to one encryption context. Adds two encrypted fields to the Task table (Social Security Numbers and Credit Cards), a read-only encryption context field, an <strong>Add Secure Info</strong> button that unhides these fields, and a <strong>Change Encryption</strong> button to change the encryption context. After activating, configure the Incident form to add the three fields.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.encryption</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- com.glide.encryption</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------</td>
<td>----</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Engine Based Notifications</td>
<td>com.glide.email_engine_notifs</td>
<td>Container for engine-based email notifications. Contains a set of default email notifications. Installed only on new z-boots.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Enhanced Web Service Provider - Common</td>
<td>com.glide.web_service_provider_v2</td>
<td></td>
<td>Active</td>
<td>false</td>
<td>com.glide.web_service_provider</td>
</tr>
<tr>
<td>E-Signature</td>
<td>com.snc.esign</td>
<td>Allows for the electronic signing of documents on both desktop and mobile. Signatories can sign with their credentials, as an acknowledgment, or as a typed or drawn e-signature.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.signaturepad, com.snc.document_management, com.snc.documentviewer</td>
</tr>
<tr>
<td>ESS Portal (implemented within Content Management)</td>
<td>com.glide.cms.extensions</td>
<td>ESS portal content management application. Demo data includes the actual ESS portal. You must request the Content Management System (CMS) application from ServiceNow personnel. Instead of activating CMS, use Service Portal for new development. Service Portal is an alternative to CMS with a refined user experience, and is active by default in the base system. See Service Portal and Content Management and Service Portal.</td>
<td>Active</td>
<td>true</td>
<td>com.glide.cms</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Event Management Connector</td>
<td>com.sn_em_connector</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Event Management Overview Homepage         | com.glideapp.report.em    | Event Management Overview Homepage                                            | Inactive| false          | • com.glideapp.report  
• com.glideapp.itom.snac                          |
<p>| Event stats                                | com.glide.stats.event     | Event stats.                                                                  | Active  | false          | com.glide.stats                                    |
| Execution Plan support for the service catalog | com.glideapp.servicecatalog | Execution Plan support for the service catalog.                              | Active  | true           | com.glide.execution_plan                         |
| Expense Line                               | com.snc.expense_line      | Core expense line table that enables cost tracking. Integrated with asset management, CMDB, cost management, and contract management. | Active  | false          |                                                   |
| Extended CMDB                              | com.snc.extended_cmdb     | Provides specialized configuration items, such as radio hardware, test equipment, and voice system hardware. | Inactive| false          | com.snc.cmdb                                      |
| External file data storage                 | com.sn.external.files     | Stores information about files in third-party systems and provides actions to manage the information. |         |                |                                                   |</p>
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facilities Move Management</td>
<td>com.snc.facilities_service_automation.move</td>
<td>This plugin enables single user move functionality as well as Enterprise Move and move planning functionality. Any floor plan aspects are not installed by default. Install the Facilities Visualization Workbench [com.snc.facilities_service_automation.fvw] plugin to use the floor plan.</td>
<td>Inactive</td>
<td>true</td>
<td>• com.snc.service_management.core</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.facilities_service_automation.fvw</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Facilities Service Management</td>
<td>com.snc.facilities_service_automation</td>
<td>Manages facilities requests and enables users to report and track requests by their location. To view requests on a floor plan, the Facilities Visualization Workbench (com.snc.facilities_service_automation.fvw) plugin is required. Integration files installed when Facilities Visualization Workbench (com.snc.facilities_service_automation.fvw) is also installed. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.service_management.core</td>
</tr>
<tr>
<td>Facilities Service Management CMS Portal (Maintenance mode only)</td>
<td>com.snc.facilities_service_automation</td>
<td>Manages facilities requests and enables users to report and track requests by their location on a floor plan. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>true</td>
<td>• com.snc.facilities_service_automation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.service_management.core.cms</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Facilities Service Management Mobile</td>
<td>com.snc.facilities_service_automation</td>
<td>Manages facilities service management mobile components.</td>
<td>Inactive</td>
<td>true</td>
<td>• com.snc.facilities_service_automation • com.snc.service_management_management</td>
</tr>
<tr>
<td>Field Normalization</td>
<td>com.snc.field_normalization</td>
<td>Provides support for cleaning up messy data through normalization and transformation.</td>
<td>Inactive</td>
<td>true</td>
<td>• com.glide.vars • com.glide.system_update_set</td>
</tr>
<tr>
<td>Field Service Capacity Management (New in Quebec)</td>
<td>com.snc.fsm_capacity_management</td>
<td>Provides capabilities to manage task capacity for groups and field agents.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.work_management</td>
</tr>
<tr>
<td>Field Service Contractor Management</td>
<td>com.snc.fsm_contractor_management</td>
<td>Enables to outsource field service tasks. Contractor companies can re assign tasks to field agents and they can work on assigned tasks.</td>
<td>Active</td>
<td>true</td>
<td>• com.snc.work_management • com.snc.outsourced_service_provider</td>
</tr>
<tr>
<td>Field Service Management</td>
<td>com.snc.work_management</td>
<td>Provides support for scheduling and managing on-location work tasks.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.snc.service_management.core • com.sn_shn • com.snc.assignment_workbench • com.snc.central_dispatch • com.snc.wo_signature_pad • com.snc.wm_questionnaire • com.snc.dynamic_scheduling</td>
</tr>
<tr>
<td>Field Service Management CMS Portal</td>
<td>com.snc.work_management</td>
<td>Enables you launch Field Service Automation and other service management applications from a single CMS page.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.snc.work_management • com.snc.service_management.core.cms</td>
</tr>
<tr>
<td>Field Service Management Configurable Dispatcher Workspace (New in Quebec)</td>
<td>com.snc.uib.fsm_dispatcher_workspace</td>
<td>Provides the FSM components and pages to support dispatcher flows on Agent Workspace.</td>
<td>Active</td>
<td>false</td>
<td>• com.snc.uib.fsm_agent_workspace • com.sn_fsm_components</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------</td>
<td>----</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
<td>--------------</td>
</tr>
</tbody>
</table>
| Field Service Management Configurable Workspace (New in Quebec) | com.snc.uib.fsm_agent_workspace | Provides the FSM components, lists, and forms to support FSM on Agent Workspace. | Active | false | • com.snc.uib.cwf_workspace  
| | | | | | • com.snc.work_management |
| Field Service Management - Customer Experience | com.snc.fsm_customer_experience | Engage customers with relevant updates on reported issues | Active | false | • com.snc.csm_fsm_integration  
| | | | | | • com.snc.notify.twilio_direct |
| Field Service Management Demo Data | com.snc.work_management.demo | Demonstration Data for Field Service Management covering the medical and telecommunication domains. NOTE: Installing this plugin adds new Configuration Item tables and relationships to the database. | Inactive | true | • com.snc.work_management  
| | | | | | • com.snc.wo_signature_pad |
| Field Service Management Geolocation Demo Data | com.snc.work_management_geolocation.demo | Enable geolocation capabilities for the Field Service Management application. | Inactive | true | com.snc.work_management.demo |
| Field Service Management Mobile | com.snc.work_management.m | Adds the Field Service Management menu to the mobile user interface. | Inactive | true | • com.snc.service_management_m  
<p>| | | | | | • com.snc.work_management |
| Field Service - Questionnaire | com.snc.wm_questionnaire | Create Questionnaires for Work Orders or Work Orders Tasks. | Inactive | false | |
| Field Service Map | com.snc.fsm_map | Displays the dispatch map for viewing agents, tasks, and agent routes. | Active | | com.snc.work_management |</p>
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field Service Management Agent Workspace</td>
<td>com.snc.agent_workspace.fsm</td>
<td>Enables field service users to manage work orders and tasks using the FSM agent workspace. This plugin activates the Agent Workspace (com.agent_workspace) plugin.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Field Service - Signature Pad</td>
<td>com.snc.wo_signature_pad</td>
<td>Create PDFs for closed work orders that include the name and signature of the customer and a summary of the completed work.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.snc.pdf_generator</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.signaturepad</td>
</tr>
<tr>
<td>Field Service Spoke</td>
<td>com.snc.field_service.spoke</td>
<td>Enables Flow Designer users to automate the creation of work orders and work order tasks and updates to existing work orders and work order tasks.</td>
<td>Inactive</td>
<td>false</td>
<td>Flow Designer - Installer (com.glide.hub)</td>
</tr>
<tr>
<td>Field Service with Project Management</td>
<td>com.snc.wm_ppm</td>
<td>Enables Field Service Management integration with the Project Management application. This plugin activates the Project Management plugin, which may require additional licenses.</td>
<td>Inactive</td>
<td>true</td>
<td>• com.snc.work_management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.financial_planning_pmo</td>
</tr>
<tr>
<td>Field Service with Project Management Demo</td>
<td>com.snc.wm_ppm_demo</td>
<td>Demonstration data for the Field Service Management integration with the Project Management application.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.snc.wm_ppm</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.work_management.demo</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.customerservice.demo</td>
</tr>
<tr>
<td>Finance Close Automation (Available in the ServiceNow Store)</td>
<td>sn_fcms</td>
<td>Reduce close risk with intelligent task automation</td>
<td>Active</td>
<td>true</td>
<td>• sn_fin</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• sn_fcms_intg</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.scope.access.restricted_caller</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Finance Common (Available in the ServiceNow Store)</td>
<td>sn_fin</td>
<td></td>
<td>Active</td>
<td>false</td>
<td>• com.snc.fiscal_calendar</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.fin_dep</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.scope.access.restricted_caller</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.web_service_insert_multiple</td>
</tr>
<tr>
<td>Finance – ERP Integration (Available in the ServiceNow Store)</td>
<td>sn_fcms_intg</td>
<td></td>
<td>Active</td>
<td>false</td>
<td>• sn_fin</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.scope.access.restricted_caller</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.web_service_insert_multiple</td>
</tr>
<tr>
<td>Finance Service Management (Maintenance mode only)</td>
<td>com.snc.finance_service_automation</td>
<td>Manages finance requests and enables users to report and track those requests. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.service_management.core</td>
</tr>
<tr>
<td>Finance Service Management Mobile</td>
<td>com.snc.finance_service_automation_m</td>
<td>Manages Finance Service Management mobile components.</td>
<td>Inactive</td>
<td>true</td>
<td>• com.snc.finance_service_automation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.service_management_m</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Charging</td>
<td>com.snc.service_charging</td>
<td>Enables financial analysts and business unit owners to measure and show charges based on the actual consumption of services. Get insight into your services and the utilization of those services by each department. Activation of this plugin on production instances may have licensing implications. Contact your ServiceNow account team for details.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.itfm_core</td>
</tr>
<tr>
<td>Modeling Engine</td>
<td>com.snc.financial_management</td>
<td>Enables financial analysts to assemble spending data, build cost models, and generate reports to show how funds are being used. Activation of this plugin on production instances may have licensing implications. Contact your ServiceNow account team for details.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.itfm_core, com.snc.financial_planning, com.snc.cost_management, com.snc.service_charging</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>Financial Management For APM</td>
<td>com.snc.financial_management</td>
<td>Enables integration of Financial Management with Application Portfolio Management providing preconfigured Cost Models. Activation of this plugin on production instances may have licensing implications. Contact your ServiceNow account team for details.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.financial_management</td>
</tr>
<tr>
<td>Financial Management for CSM</td>
<td>com.snc.financial_management</td>
<td>Plugins for Customer Service Management and Field Service Management provide integration with the Financial Management application. These plugins add cost allocations for the CSM and FMS applications as well as dashboards and reports. Financial administrators can use these cost allocations on the Financial Management workbench to allocate, track, and report on expenses.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.financial_management com.sn_customerservice</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Financial Management For FSM | com.snc.financial_management_for_fsm | Enables Integration of Financial Management with Field Service Management providing preconfigured Cost Models and a dashboard. Activation of this plugin on production instances may have licensing implications. Contact your ServiceNow account team for details. | Inactive | true           | • com.snc.financial_management  
• com.snc.work_management  
• com.snc.pa  
• com.snc.pa_fm.fsm |
| Financial Management for SPM | com.snc.financial management_for_spm | Enables Integration of Financial Management with Service Portfolio Management providing preconfigured Cost Models. Activation of this plugin on production instances may have licensing implications. Contact your ServiceNow account team for details. | Active | true           | • com.snc.financial_management  
• com.spm_owner_workspace |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Planning</td>
<td>com.snc.financial_planning</td>
<td>Preconfigured Financial Plan Definition and all its artifacts which enables Financial Analysts to plan for costs, make forecasts, and evaluate actual expenses versus planned expenses. Planning takes into consideration a wide range of items in your infrastructure, including assets, labor, and the configuration items in the CMDB. Activation of this plugin on production instances may have licensing implications. Contact your ServiceNow account team for details.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.financial_planning</td>
</tr>
<tr>
<td>Financial Services Card Operations (Available in the ServiceNow Store)</td>
<td>sn_bom_credit_card</td>
<td>Application specific to Card Operations focused on different customer requests in the card service domain and is part of the overall Financial Services Operations product.</td>
<td>Inactive</td>
<td>true</td>
<td>• com.snc.csm_case_types</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.sn_cs_sm_request</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• sn_bom</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• sn_bom_credit_asmt</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• sn_bom_document</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Financial Services Credit Assessment</td>
<td>sn_bom_credit_asmt</td>
<td>Application for Credit Assessment which is a shared service with many other service domains such as Card Operations. This is part of the overall Financial Services Operations product. This application is automatically installed when you install the Financial Services Card Operations application.</td>
<td>Inactive</td>
<td>true</td>
<td>sn_bom</td>
</tr>
<tr>
<td>Financial Services Document Management</td>
<td>sn_bom_document</td>
<td>Application for Document Services which is a shared service with many other service domains such as Card Operations. This is part of the overall Financial Services Operations product. This application is automatically installed when you install the Financial Services Card Operations application.</td>
<td>Inactive</td>
<td>true</td>
<td>sn_bom</td>
</tr>
</tbody>
</table>
| Financial Services Business Loan Operations (Available in the ServiceNow Store) | sn_bom_loan_b2b | Application specific to Business Loan Operations focused on different loan requests and exceptions in the loan service domain and is part of the overall Financial Services Operations product. | Inactive | true          | • com.snc.csm_case_types
• com.sn_cs_sm_request
• sn_bom
• sn_bom_credit_asmt
• sn_bom_document |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
</table>
| Financial Services Personal Loan Operations (Available in the ServiceNow Store) | sn_bom_loan | Application specific to Personal Loan Operations focused on different loan requests and exceptions in the loan service domain and is part of the overall Financial Services Operations product. | Inactive | true | • com.snc.csm_case_types  
  • com.sn_cs_sm_request  
  • sn_bom  
  • sn_bom_credit_asmt  
  • sn_bom_document |
| Financial Services Payment Operations (Available in the ServiceNow Store) | sn_bom_payment | Application specific to Payment Operations focused on customer payment inquiries, claims, and refunds. This application is part of the overall Financial Services Operations product. | Inactive | true | • com.snc.csm_case_types  
  • com.sn_cs_sm_request  
  • sn_bom |
| Financial Services Operations Core (Available in the ServiceNow Store) | sn_bom | Core application for Financial Services Operations product which includes the data model for Financial Accounts, Financial Products and Financial Transactions. This application is automatically installed when you install any of the Financial Services Operations applications. | Inactive | true | • com.snc.install_base  
  • com.sn_customerservice  
  • sn_ind |
| FSO Process Optimization Content Pack (Available in the ServiceNow Store) | sn_bom_po | Provides Process Optimization capabilities to Financial Services Operations applications. | Inactive | false | • com.sn_process_optimization  
  • sn_bom |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
</table>
| Performance Analytics Content Pack for FSO (Available in the ServiceNow Store) | sn_bom_pa      | Provides Performance Analytic capabilities to Financial Services Operations applications.                                                                                                                     | Inactive | false          | • com.snc.pa  
• sn_bom |
| Fiscal Calendar                          | com.snc.fiscal_calendar | Enables to generate and manage different kinds of Fiscal calendar which is used in various Financial applications. Activation of this plugin on production instances may have licensing implications. Contact your ServiceNow account team for details. | Inactive | false          | com.glide.dynamic_operands.datetime |
| Fixed Asset                              | com.snc.fixed_asset | Core fixed asset tracking                                                                                                                                                                                    | Active  | false          |                                      |
| Fixed Costs                              | com.snc.fixed_costs | Fixed Costs                                                                                                                                                                                                 | Active  | false          | com.glide.metrics                    |
| Flow Client                              | com.glide.hub.flow.client | The client side API for interacting with flows, subflows, and actions                                                                                                                                       | Active  | false          | com.glide.hub.scriptable.plan.runners |
| Flow Designer - Designer                 | com.glide.hub.designer | Flow Designer - Designer                                                                                                                                                                                     | Active  | false          | com.glide.hub.designer_backend.suite |
• com.glide.dashboards |
• com.glideapp.dashboards |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Flow Designer - Flow Engine Reporting</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.hub.flow_reporting.dashboard</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Outbound Tracking</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Flow Designer Action Step - Log</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Flow Designer Action Step - Script</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Flow Designer Action Step - CRUD</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.hub.action_step.notification</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Flow Designer Action Step - CORE</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.hub.action_step.service_catalog</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.hub.designer_backend.model</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Flow Designer Action Step - Email</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Flow Designer System Level Actions</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Connect Spoke for Flow Designer</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Flow Designer - Designer</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.hub.action_step.email_header</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.hub.action_step.look_up_email_attachments</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• App Dependency Client</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flow Designer Action Step -</td>
<td>com.glide.hub.action_step.core</td>
<td>Action Step - Core operations on GlideRecord.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.hub.action_step.template</td>
</tr>
<tr>
<td>CORE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CRUD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.email.service</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.hub.action_step.email_template</td>
</tr>
<tr>
<td>Log</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------</td>
<td>----</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
<td>--------------</td>
</tr>
</tbody>
</table>
| Flow Designer Action Step - Notification | com.glide.hub.action_step.notification | Action steps for notifications. | Active | false | • com.glide.notification  
• com.glide.hub.action_step.template |
| Flow Designer Action Step Template | com.glide.hub.action_step.template | Template Design Time components. | Active | false | |
| Flow Designer Action Trigger | com.glide.hub.flow_trigger | Action plans that map a Trigger (Record, Email, REST) to an Action. | Active | false | com.glide.hub.flow_engine |
| Flow Designer Designer Backend | com.glide.hub.designer_backend | Suite of plugins necessary to support the Flow Designer Designer App. | Active | false | • com.glide.hub.action_step.log  
• com.glide.hub.action_step.script  
• com.glide.hub.action_step.crud  
• com.glide.hub.action_step.email  
• com.glide.hub.action_step.notification  
• com.glide.hub.action_step.core  
• com.glide.hub.designer_backend.model  
• com.glide.hub.action_type.system |
• com.glide.hub.flow_engine  
• com.glide.hub.flow_trigger  
• com.glide.hub.flow_reporting  
• com.glide.hub.action_step.template |
<p>| Flow Designer Scriptable Plan Runner API's | com.glide.hub.scriptable.plan_runner | Suite of API's needed to run flows, subflows, and actions through script. | Active | false | com.glide.hub.flow_engine |</p>
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow Designer support for the Service Catalog</td>
<td>com.glideapp.servicecatalog.flow_designer</td>
<td>Service Catalog Flow Designer</td>
<td>Active</td>
<td>true</td>
<td>com.glide.hub.flow_trigger.catalog</td>
</tr>
<tr>
<td>Flow Designer System Level Actions</td>
<td>com.glide.hub.action_type.system.action_type</td>
<td>Action Type Definitions for low-level functions such as GlideRecord operations.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.hub.designer_backend.model</td>
</tr>
<tr>
<td>Form Designer</td>
<td>com.glide.ui.ng.fd</td>
<td>Form Designer</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Form Personalization</td>
<td>com.glide.ui.personalize_form.self</td>
<td>Enables users to personalize the layout for any form view.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.ui.doctype</td>
</tr>
<tr>
<td>FSM Agent Workspace</td>
<td>com.snc.agent_workspace.fsm</td>
<td>Enables users to manage work orders and tasks within the agent workspace.</td>
<td>Inactive</td>
<td>false</td>
<td>com.agent_workspace</td>
</tr>
<tr>
<td>Fullcalendar Library</td>
<td>com.snc.fullcalendar</td>
<td>Fullcalendar library v2.5.0.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Geolocation</td>
<td>com.snc.geolocation</td>
<td>Uses Google Maps to track users, plan efficient routes between locations, and assist in finding accurate travel times. The system locates users from latitude and longitude information provided by their mobile devices.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Github Spoke</td>
<td>com.sn.github.spoke</td>
<td>The GitHub Spoke for IntegrationHub provides actions that a Process Analyst can use when designing flows. The actions allow them to automate GitHub tasks.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Gitlab Spoke</td>
<td>com.sn.gitlab.spoke</td>
<td>The GitLab Spoke for IntegrationHub provides actions that a Process Analyst can use when designing flows. The actions allow them to automate Gitlab.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Glide Conversation Server</td>
<td>com.glide.cs</td>
<td>Glide Conversation Server.</td>
<td>Inactive</td>
<td>true</td>
<td>• com.glide.connect.support</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.cs.branding</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.cs.live_agent_settings</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.cs.sn-va-web-client-app</td>
</tr>
<tr>
<td>Glide Conversation Server Adapters</td>
<td>com.glide.cs.adapter</td>
<td>Glide Conversation Server Adapters</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.cs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.external.app</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.channelproxy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.bot_install_ui</td>
</tr>
<tr>
<td>Glide Metadata</td>
<td>com.glide.metadata</td>
<td>Core metadata support.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.metadata</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.metadata_tree</td>
</tr>
<tr>
<td>Glide Metadata Delete</td>
<td>com.glide.metadata_delete</td>
<td>Core metadata delete support.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.metadata</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.metadata_tree</td>
</tr>
<tr>
<td>Glide Virtual Agent</td>
<td>com.glide.cs.chatbot</td>
<td>Activates the Virtual Agent framework and the other necessary plugins.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.cs.chatbot.lite</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.cs.custom.adapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.cs.nlu.topics</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.nlu.intent.discovery</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.nlu.ibmwatson.intent.discovery</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.nlu.msluis.intent.discovery</td>
</tr>
<tr>
<td>Glide Virtual Agent Lite</td>
<td>com.glide.cs.chatbot.lite</td>
<td>Activates the lite version of the Virtual Agent bot platform and other necessary plugins.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.cs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.va.sp_widgets</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.cs.adapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.cs.settings</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.cs.topics</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.service-portal.agent-chat</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.cs.topic_blocks</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.conversation_builder</td>
</tr>
<tr>
<td>Global Application File Management</td>
<td>com.snc.global_app_files</td>
<td>UI components and utilities for managing application files in the global scope.</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.scripted_rest_services</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.ui.ng</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Google Calendar Spoke</td>
<td>com.sn.gcalendar.spoke</td>
<td>The Google Calendar Spoke for IntegrationHub provides actions that a Process Analyst can use when designing flows. The actions allow them to automate Google Calendar.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Google Maps Plugin</td>
<td>com.glideapp.google_maps</td>
<td>Allows the display of Google Maps within the product as map pages.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.ui.ng • com.glide.rest.service</td>
</tr>
<tr>
<td>Granular Delegation</td>
<td>com.glide.granular_service_delegation</td>
<td>Delegate specific assignments and approvals to another user for a period of time.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>GraphQL Schema for Contextual Search</td>
<td>com.snc.contextual_search.graphql</td>
<td>Provides GraphQL schema for contextual search services</td>
<td>true</td>
<td>false</td>
<td>com.glide.graphql</td>
</tr>
<tr>
<td>GraphQL Schema for Knowledge in Contextual Search/Application Portfolio Management</td>
<td>com.snc.knowledge3.graphql</td>
<td>Provides GraphQL schema for contextual search sources like Knowledge</td>
<td>true</td>
<td>false</td>
<td>com.snc.contextual_search.graphql</td>
</tr>
<tr>
<td>GRC: Audit Management</td>
<td>com.sn_audit</td>
<td>The GRC: Audit Management application provides a centralized process for Internal Audit teams to automate the complete audit life cycle. Project driven audits allow auditors to quickly scope engagements, conduct fieldwork, collect control evidence, and track audit observations.</td>
<td>Inactive</td>
<td>true</td>
<td>com.sn_grc • com.glide.ui.ng • com.snc.common_workbench</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>GRC: Business Continuity Management – Components</td>
<td>sn_bcm_components</td>
<td>Provides seismic components for Business Continuity Management application</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>GRC: Business Continuity Management – Core</td>
<td>sn_bcm</td>
<td>Provides capabilities to configure the core data and workspace that are required for the business continuity management applications.</td>
<td>Active</td>
<td>true</td>
<td>com.snc.app_bcm_components</td>
</tr>
<tr>
<td>GRC: Business Continuity Planning</td>
<td>sn_bcp</td>
<td>Provides capabilities for business continuity management teams to create, review, and approve business continuity and disaster recovery plans.</td>
<td>Active</td>
<td>true</td>
<td>com.snc.bcm.app_bcm_components, com.snc.document_templates</td>
</tr>
<tr>
<td>GRC: Business Impact Analysis</td>
<td>sn_bia</td>
<td>Provides structured workflows for business continuity management teams to assess the impact of a disruption to critical resources such as business processes, applications, and locations.</td>
<td>Active</td>
<td>true</td>
<td>com.snc.bcm.app_bcm_core</td>
</tr>
<tr>
<td>GRC: Crisis Management</td>
<td>sn_recovery</td>
<td>Provides capabilities for business continuity management teams to activate business continuity plans during plan exercises and actual crisis events.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.bcm.app_bcm_planning</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>GRC: Compliance UCF</td>
<td>com.sn_comp_ufc</td>
<td>The GRC: Compliance UCF plugin is an add-on that provides GRC: Policy and Compliance Management with the capability to download regulatory content and common controls from the Unified Compliance Framework (UCF).</td>
<td>Inactive</td>
<td>false</td>
<td>com.sn_compliance</td>
</tr>
</tbody>
</table>
| GRC: GDPR DPIA Accelerator            | com.sn_irm_gdpr_dpiaccessor  | Use case accelerator for GDPR Data Protection Impact Assessment.                                                                                                                                           | Inactive | false          | • com.snc.grc_audit_dep  
  • com.snc.grc_profile_dep  
  • com.snc.grc_policy_dep  
  • com.snc.grc_risk_dep |
| GRC: Mobile                           | com.sn_grc_mobile | There are two GRC core applications that are viewed on the GRC Mobile app: Policy and Compliance Management and Risk Management. There are two GRC core applications that are viewed on the GRC Mobile app: Policy and Compliance Management and Risk Management. | Inactive | false          | com.glide.sg ,  
  com.glide.sg.agent_native_client |
<p>| GRC: Performance Analytics Integration | com.sn_grc_pa | GRC: Performance Analytics Integration enables risk and compliance managers to continuously monitor key risk and control indicators using the advanced reporting capabilities provided by Performance Analytics. | Inactive | false          | com.sn_grc |</p>
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
</table>
| GRC: Policy and Compliance Management      | com.sn_compliance | The GRC: Policy and Compliance Management application provides a centralized process for creating and managing policies, standards, and internal control procedures that are cross-mapped to external regulations and best practices. The application provides structured workflows for the identification, assessment, and continuous monitoring of control activities. | Inactive | true           | • com.sn_grc  
• com.snc.comp_attest |
| GRC: Predictive Intelligence               | com.sn_grc_pred_intel | Enables customers to utilize the machine learning algorithms for a wide variety of GRC use cases such as Issue Assignment. This plugin may require a separate license. Contact ServiceNow for details. | Inactive | false          | • com.glide.platform_ml  
• com.sn_grc |
| GRC: GRC Profile Dependencies              | com.snc.grc_profile_dep | Installs all the dependent plugins required to support the GRC Profile application.                                                                                                                                 | Active | false          | • com.snc.grc.common  
• com.snc.planned_task_v2 |
| GRC: Regulatory Change Management          | com.sn_grc_reg_change | The Regulatory Change Management application enables customers to check upcoming regulatory changes, assess their impact, and implement risk and compliance-related changes, ensuring overall regulatory compliance. | Active | false          | • com.snc.grc_policy_dep  
• com.snc.grc_profile_dep  
• com.snc.grc_risk_dep  
• com.glide.hub.action_step.sftp  
• com.glide.hub.action_type.datastream  
• com.glide.hub.integration.runtime |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRC integration with Thomson Reuters</td>
<td>com.sn_grc_int_tr</td>
<td>Use the GRC integration with Thomson Reuters Regulatory Intelligence application to integrate with the Thomson Reuters platform and to consume the Thomson Reuters Regulatory Intelligence (TRRI) feeds into your ServiceNow instance.</td>
<td>Active</td>
<td>true</td>
<td>• com.snc.grc_profile_dep • com.snc.grc_policy_dep • com.snc.grc_risk_dep</td>
</tr>
<tr>
<td>Regulatory Intelligence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GRC: RSS Feed Integration to Regulatory</td>
<td>com.sn_grc_rcm_rssfeed</td>
<td>The GRC: RSS Feed Integration to Regulatory Change application helps keep track of regulatory changes and other updates by enabling you to subscribe to public RSS feeds and bringing that data in ServiceNow.</td>
<td>Active</td>
<td>true</td>
<td>com.sn_grc_reg_change</td>
</tr>
<tr>
<td>Change</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>GRC: Advanced Risk</td>
<td>com.sn_risk_advanced</td>
<td>As a decision-maker, at any level of the business, you can view up-to-date information regarding your organization's risk posture. Link intermediate risk statements to risks, as well as enterprise-level risk statements. Your risk management team can provide a rollup of risk statements and scores from the most granular risk to the highest enterprise-level risk statement. Additionally, as a risk manager, you can monitor risk events, relate them to existing risks, perform root-cause analysis, and track all remediation tasks.</td>
<td>Active</td>
<td>true</td>
<td>• com.snc.grc_profile_dep • com.snc.grc_risk_dep</td>
</tr>
<tr>
<td>GRC: Risk Management</td>
<td>com.sn_risk</td>
<td>The GRC: Risk Management application provides a centralized process to identify, assess, respond to, and continuously monitor Enterprise and IT risks that may negatively impact business operations. The application also provides structured workflows for the management of risk assessments, risk indicators, and risk issues.</td>
<td>Inactive</td>
<td>true</td>
<td>• com.sn_grc • com.snc.risk_asmt</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------</td>
<td>----</td>
<td>-------------</td>
<td>-------</td>
<td>---------------</td>
<td>--------------</td>
</tr>
</tbody>
</table>
| GRC: Risk Management Dependencies | com.snc.grc_vrm_dep | Installs all the dependent plugins required to support the GRC Risk Management application. | Active | false | • com.snc.grc_profile_dep  
• com.snc.risk_asmt |
| GRC: SIG Questionnaire Integration | com.sn_sig_asmt | The GRC: SIG Questionnaire Integration plugin installs the Shared Assessments Standardized Information Gathering (SIG) questionnaire for use with the GRC: Vendor Risk Management application. | Inactive | true | • com.snc.assessment_core  
• com.sn_vdr_risk_asmt  
• com.snc.sig_asmt_core  
• com.snc.document_management |
| GRC: Vendor Risk Management | com.sn_vdr_risk_asmt | The GRC: Vendor Risk Management application allows risk management stakeholders to identify, assess, and manage risk across the vendor ecosystem. | Inactive | true | • com.sn_comp_asmt  
• com.snc.vendor_core  
• com.sn_grc  
• com.snc.vdr_risk_asmt_designer  
• com.snc.vendor_portal |
| GRC: Vendor Risk Management Dependencies | com.snc.grc_vrm_dep | Installs all the dependent plugins required to support the GRC Vendor Risk Management application. | Active | false | • com.snc.grc_profile_dep  
• com.snc.vdr_risk_asmt_designer  
• com.snc.vendor_core  
• com.snc.sig_asmt_core  
• com.snc.assessment_core  
• com.snc.document_management  
• com.snc.vendor_portal |
| GRC: Virtual Agent | com.sn_grc_virtual_agent | The GRC: Virtual Agent provides chat bot functionality for common GRC operations. | | | |

© 2021 ServiceNow, Inc. All rights reserved. ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRC: Workbench</td>
<td>com.sn_grc_workbench</td>
<td>The GRC Workbench utilizes CMDB information to show the upstream and downstream relationships across all applications. These relationships enable consistent risk mapping and modeling across the enterprise. The GRC Workbench does not work with Legacy GRC.</td>
<td>Inactive</td>
<td>false</td>
<td>com.sn_grc</td>
</tr>
<tr>
<td>Guided Application Creator</td>
<td>com.glide.sn-guided-app-creator</td>
<td>Enables users to set up custom business applications that are immediately ready to use.</td>
<td>Active</td>
<td>false</td>
<td>com.sn_appcreator</td>
</tr>
<tr>
<td>Guided Decisions (Maintenance mode only)</td>
<td>com.snc.guided_decisions</td>
<td>Enables the framework and execution engine for creating guided decisions.</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.decision_table&lt;br&gt;• com.snc.guided_decisions_guidance&lt;br&gt;• com.glide.hub</td>
</tr>
<tr>
<td>Guided Decisions - Guidance (Maintenance mode only)</td>
<td>com.snc.guided_decisions_guidance</td>
<td>Enables the framework for creating a guidance for guided decisions.</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.hub&lt;br&gt;• com.snc.guided_decisions_guidance_global</td>
</tr>
<tr>
<td>Guided Decisions - Guidance Global Entities (Maintenance mode only)</td>
<td>com.snc.guided_decisions_guidance_global</td>
<td>This plugin is loaded as dependant of Guided Decisions Guidance to access global entities.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Guided Decision - Next Best Action (New in Quebec)</td>
<td>com.snc.next_best_action</td>
<td>Recommends relevant actions like Guided Decisions for a given context. The plugin enables defining rules to recommend Next Best Actions.</td>
<td>Active</td>
<td>false</td>
<td>com.sn_next_best_action_list</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------------------------</td>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Guided Decisions for Playbook in Workspace</td>
<td>com.snc.guided_decisions_playbook</td>
<td>Enables capturing instance types, definitions, and UI components for the display of guided decisions in a playbook on Workspace.</td>
<td>Active</td>
<td>false</td>
<td>• com.snc.guided_decisions &lt;br&gt;• com.snc.guided_decisions_guidance &lt;br&gt;• com.glide.playbook_experience.config</td>
</tr>
<tr>
<td>Guided Setup Configuration (New in Quebec)</td>
<td>com.glide.guided_setup_config</td>
<td>Provides customers with a configuration on the Guided Setup Content.</td>
<td>Active</td>
<td>false</td>
<td>• com.snc.guided_setup &lt;br&gt;• com.snc.cmdb</td>
</tr>
<tr>
<td>Guided Setup for CMDB</td>
<td>com.snc.cmdb.guided_setup</td>
<td>Provides customers with a visual guidance to configure CMDB. Requires UI16.</td>
<td>Active</td>
<td>false</td>
<td>• com.snc.guided_setup &lt;br&gt;• com.snc.cmdb</td>
</tr>
<tr>
<td>Guided Setup for Performance Analytics</td>
<td>com.snc.pa.guided_setup</td>
<td>Provides customers with visual guidance to configure Performance Analytics. Requires UI16.</td>
<td>Active</td>
<td>false</td>
<td>• com.snc.guided_setup &lt;br&gt;• com.snc.pa &lt;br&gt;• com.glideapp.dashboards</td>
</tr>
<tr>
<td>Guided Setup for ServiceNow Flow Designer (New in Quebec)</td>
<td>com.glide.hub.flow_designer_guided_tours</td>
<td>Guided tour instructing users on how to start creating a flow.</td>
<td>Active</td>
<td>false</td>
<td>• com.glideapp.ui_components &lt;br&gt;• com.glide.scripted_rest_services &lt;br&gt;• com.glide.embedded_help &lt;br&gt;• com.glide.scoped_analytics_framework</td>
</tr>
<tr>
<td>Guided Setup Framework</td>
<td>com.snc.guided_setup</td>
<td>Provides customers with visual guidance to configure ServiceNow applications.</td>
<td>Active</td>
<td>false</td>
<td>• com.glideapp.ui_components &lt;br&gt;• com.glide.scripted_rest_services &lt;br&gt;• com.glide.embedded_help &lt;br&gt;• com.gl...</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------</td>
<td>---------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Guided Tour Designer</td>
<td>com.glide.sn_tourbuilder</td>
<td>ServiceNow Guided Tour Designer, aka GTD is a simplified way to create a guided tour. It provides easy to use, drag and drop interface to quickly build guided tours without writing any code. You can add, delete, modify, reorder steps as well as test the tour by previewing it.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Guided Tours</td>
<td>com.glide.guided_tours</td>
<td>A guided tour provides a walk-through of a procedure in a UI page. Administrators can develop customized guided tours to assist users with specific business processes within an organization.</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.ui.hopscotch</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.embedded_help</td>
</tr>
<tr>
<td>Hardware Asset Management</td>
<td>com.sn_hamp</td>
<td>Hardware Asset Management Professional focuses on driving automation and prescriptive, standard practices for managing physical hardware assets throughout the end-to-end asset lifecycle from acquisition through disposition.</td>
<td>Active</td>
<td>false</td>
<td>com.sn_hwnorm</td>
</tr>
<tr>
<td>(Maintenance mode only)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Hardware Model Normalization</td>
<td>com.sn_hwnorm</td>
<td>Hardware normalization is a net new app planned for limited access in the Orlando release. This feature will enable customers with ITAM hardware normalization plugin to received standardized content to normalize records for IT hardware manufacturers, models and model lifecycles.</td>
<td>Inactive</td>
<td>true</td>
<td>• com.snc.model</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.data_services_canonicalization</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.sn_glidequery</td>
</tr>
<tr>
<td>Health Log Analytics Core</td>
<td>com.glideapp.itom.occultus</td>
<td>Essential components for Health Log Analytics scoped application.</td>
<td>false</td>
<td></td>
<td>• com.glide.indexed-docstore.es</td>
</tr>
<tr>
<td>(New in Quebec)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.clotho</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.itom.jutils</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.services</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.auth.mutual</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glideapp.itom.snac</td>
</tr>
<tr>
<td>Health Log Analytics Viewer</td>
<td>com.sn-log-viewer</td>
<td></td>
<td>false</td>
<td></td>
<td>• com.glide.role_management</td>
</tr>
<tr>
<td>(New in Quebec)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High Security Settings</td>
<td>com.glide.high_security</td>
<td>Enables a high-security environment, including high-security system properties and access controls.</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.role_management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>History Sets</td>
<td>com.glide.history_set</td>
<td>Maintains sys_history_set and sys_history_line tables to view a record's audit, email, and relationship data in a table format.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>History Walker</td>
<td>com.glide.history_walker</td>
<td>Provides script access to History Walker</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Homepage Splash Page</td>
<td>com.glideapp.home.splash_page</td>
<td>Provides a splash page for homepages. Upon logging in, instead of going to home.do, users go to a splash page that gives them the ability to cancel the home page transaction. This is useful when homepages take a long time to load.</td>
<td>Active</td>
<td>false</td>
<td>com.glideapp.home</td>
</tr>
<tr>
<td>Hopscotch</td>
<td>com.glide.ui.hopscotch</td>
<td>Hopscotch is a framework to make it easy for developers to add product tours to their pages. Hopscotch accepts a tour JSON object as input and provides an API for the developer to control rendering the tour display and managing the tour progress. To learn more about Hopscotch and the API, check out <a href="http://linkedin.github.io/hopscotch">http://linkedin.github.io/hopscotch</a>.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>HTML Sanitizer</td>
<td>com.glide.htmlsanitizer</td>
<td>Automatically cleans up HTML markup in all HTML fields to remove unwanted code to protect against security concerns such as cross-site scripting attacks.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Human Resources Application: Core CMS</td>
<td>com.snc.hr.core.cms</td>
<td>Provides case and knowledge management for HR. Standardizes the documentation, interaction, and fulfillment of employee inquiries and requests while having visibility into the quantity and type of cases coming in.</td>
<td>Inactive</td>
<td>true</td>
<td>• com.glide.country</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.db_images</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.appview</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.document_management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.knowledge3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.pdf_generator</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.sc_catalog_manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.signaturepad</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.skills_management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.task_activity</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.matching_rule</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.hr.scoped_security</td>
</tr>
</tbody>
</table>

**Warning:**
Be sure that you do not have plugin Human Resources Application: Core activated. This plugin is a new HR application that duplicates some functionality in Human Resources Application: Core. If you have any questions about this plugin, contact your ServiceNow account manager.

Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human Resources Scoped App: Integrations</td>
<td>com.sn_hr_integrations</td>
<td>HR Integration provides the ability to integrate with multiple third-party HR systems for the scoped version of HRSM. HR Integration pushes HR profile information from HRSM to a third-party HR application and pulls HR profile information from a third-party HR application to HRSM.</td>
<td>Inactive</td>
<td>true</td>
<td>com.glide.scope.access.restricted_caller</td>
</tr>
<tr>
<td>Human Resources Scoped App: Lifecycle Events</td>
<td>com.sn_hr_lifecycle_events</td>
<td>Activates the Lifecycle Event module for HR. Combined with other licensed applications, provides a full-service, employee journey experience such as onboarding or parental leave of absence for employees and those managing the process.</td>
<td>Inactive</td>
<td>true</td>
<td>com.sn.hr.core &lt;br&gt; com.sn_hr_service_portal</td>
</tr>
<tr>
<td>Human Resources Scoped App: Lifecycle Events for Enterprise</td>
<td>com.sn_hr_lifecycle_enthelene</td>
<td>Human Resources Scoped App: Lifecycle Events for Enterprise enables you to automate onboarding and other employee lifecycle events that span across multiple departments such as IT, Facilities, Finance, and Legal.</td>
<td>Inactive</td>
<td>true</td>
<td>com.sn_hr_lifecycle_events &lt;br&gt; com.sn_hr_core &lt;br&gt; com.sn_hr_service_portal &lt;br&gt; com.sn_hr_onboarding &lt;br&gt; com.snc.businessroles</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------</td>
<td>----------------------------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Human Resources Scoped App: Mobile</td>
<td>com.sn_hr_mobile</td>
<td>Activates the Mobile module for HR. Combined with Mobile Employee Experience Native Application plugin, items related to HR will be shown in the native mobile application.</td>
<td>Active</td>
<td>true</td>
<td>• com.glide.mobile-employee</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.sn_hr_core</td>
</tr>
<tr>
<td>Human Resources Scoped App: Mobile Onboarding</td>
<td>com.sn_hr_onboarding</td>
<td>Enable your new hires to complete onboarding to-dos, ask questions, and view relevant content using the new Mobile Onboarding application.</td>
<td>Inactive</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------</td>
<td>----</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Human Resources Scoped App: Parental Journey</td>
<td>com.sn_hr_parental_journey</td>
<td>Activates the Employee Journey for Parental Leave of Absence. Combined with other licensed applications, provides a full-service, parental leave of absence experience for employees and those managing the process.</td>
<td>Active</td>
<td>true</td>
<td>com.sn_hr_lifecycle_events</td>
</tr>
<tr>
<td>Human Resources Scoped App: Security</td>
<td>com.sn.hrScoped_security</td>
<td>Activation of this plugin on production instances requires a separate license. Contact ServiceNow for details. Human Resources Scoped App: Core plugin requires this plugin.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.service-portal</td>
</tr>
<tr>
<td>Human Resources Scoped App: Service Portal</td>
<td>com.sn.hr_service_portal</td>
<td>Provides a single place for employees to quickly and easily get all the HR services they need.</td>
<td>Inactive</td>
<td>true</td>
<td>• com.sn_hr_core • com.glide.connect.support</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------</td>
<td>----</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
<td>--------------</td>
</tr>
</tbody>
</table>
| Human Resources Scoped App: Virtual Agent Conversations | com.sn_hr_virtual_agent | Activates a conversational bot platform for providing user assistance through conversations within a messaging interface for HR. | Active | false | • com.glide.cs
• com.sn_hr_core
• com.glide.cs.chatbot
• com.glide.cs.sn-va-web-client-app
• com.sn_hr_service_portal
• com.glide.va.sp_widgets |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
</table>
| Human Resources Scoped App: Workspace       | sn_hr_agent_workspace                   | Activates a configurable service desk application that provides agents with an integrated and graphically intuitive user experience for HR. |       | false         | • com.agent_workspace  
• com.snc.sn_lookup_and_verify_config  
• com.sn_hr_core                                                                |
<p>| I18N: Brazilian Portuguese Translations     | com.snc.i18n.brazilian_portuguese       | Internationalization plugin for language internationalization. Provides Brazilian Portuguese. | Inactive | false | com.glide.i18n                                                             |
| I18N: Czech Translations                    | com.snc.i18n.czech                      | An Internationalization plugin for language internationalization. Provides Czech. | Inactive | false | com.glide.i18n                                                             |
| I18N: Dutch Translations                    | com.snc.i18n.dutch                      | An Internationalization plugin for language internationalization. Provides Dutch. | Inactive | false | com.glide.i18n                                                             |
| I18N: Finnish Translations                  | com.snc.i18n.finnish                    | An Internationalization plugin for language internationalization. Provides Finnish. | Inactive | false | com.glide.i18n                                                             |</p>
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>I18N: French - Canada Translations</td>
<td>com.snc.i18n.french-canada</td>
<td>An Internationalization plugin for language internationalization. Provides French - Canadian.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td>I18N: French Translations</td>
<td>com.snc.i18n.french</td>
<td>An Internationalization plugin for language internationalization. Provides French.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td>I18N: German Translations</td>
<td>com.snc.i18n.german</td>
<td>An Internationalization plugin for language internationalization. Provides French.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td>I18N: Hebrew Translations</td>
<td>com.snc.i18n.hebrew</td>
<td>An Internationalization plugin for language internationalization. Provides Hebrew.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td>I18N: Hungarian Translations</td>
<td>com.snc.i18n.hungarian</td>
<td>An Internationalization plugin for language internationalization. Provides Hungarian.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td>I18N: Internationalization</td>
<td>com.glide.i18n</td>
<td>An Internationalization plugin for language internationalization. Provides the elements necessary for translating an instance without any translation preloaded.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.system_import_set</td>
</tr>
<tr>
<td>I18N: Internationalization Translation helper</td>
<td>com.glide.i18n.translation_helper</td>
<td>Modules and import set maps to merge all languages into one table for translation maintenance.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td>I18N: Italian Translations</td>
<td>com.snc.i18n.italian</td>
<td>An Internationalization plugin for language internationalization. Provides Italian.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------</td>
<td>---------------</td>
<td>--------------</td>
</tr>
<tr>
<td>I18N: Japanese Translations</td>
<td>com.snc.i18n.japanese</td>
<td>An Internationalization plugin for language internationalization. Provides Japanese.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td>I18N: Knowledge Management Internationalization Plugin v2</td>
<td>com.glideapp.knowledge.i18n</td>
<td>Activating internationalization plugins for any of the available languages automatically activates this plugin. This plugin helps create and maintain translations of an article in various languages in a way that is easy to manage translations while authoring as well as viewing articles.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glideapp.knowledge.i18n, com.glide.i18n</td>
</tr>
<tr>
<td>I18N: Korean Translations</td>
<td>com.snc.i18n.korean</td>
<td>Korean Translations</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td>I18N: Polish Translations</td>
<td>com.snc.i18n.polish</td>
<td>An Internationalization plugin for language internationalization. Provides Polish.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td>I18N: Portuguese Translations</td>
<td>com.snc.i18n.portuguese</td>
<td>An Internationalization plugin for language internationalization. Provides Portuguese.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td>I18N: Russian Translations</td>
<td>com.snc.i18n.russian</td>
<td>An Internationalization plugin for language internationalization. Provides Russian.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td>I18N: Simplified Chinese Translations</td>
<td>com.snc.i18n.chinese</td>
<td>An Internationalization plugin for language internationalization. Provides Simplified Chinese.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>I18N: Spanish Translations</td>
<td>com.snc.i18n.spanish</td>
<td>An Internationalization plugin for language internationalization. Provides Spanish.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td>I18N: Thai Translations</td>
<td>com.snc.i18n.thai</td>
<td>An Internationalization plugin for language internationalization. Provides Thai.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td>I18N: Traditional Chinese Translations</td>
<td>com.snc.i18n.traditional_chinese</td>
<td>An Internationalization plugin for language internationalization. Provides Traditional Chinese.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td>I18N: Turkish Translations</td>
<td>com.snc.i18n.turkish</td>
<td>An Internationalization plugin for language internationalization. Provides Turkish.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td>IBM Watson Assistant Integration</td>
<td>com.glide.cs.ibm.watson.assistant.topic</td>
<td>Enables the IBM Watson Assistant topic to run an IBM skill (conversation) created in IBM Watson with the Assistant V1 API. The topic runs in the Virtual Agent web client.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>IBM Watson Assistant Integration V2</td>
<td>com.glide.cs.ibm.watson.assistant.v2.topic</td>
<td>Enables the IBM Watson Assistant Chat Integration to run a dialog skill (conversation) created in IBM Watson with the Assistant V2 API. The topics runs in the Virtual Agent web client.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
<td>---------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IBM Watson Translator Service Spoke</td>
<td>com.glide.ibm_translation_spoke</td>
<td>Using IBM translation services, it adds ability to translate text from one language to another and detect the language of text.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.hub.integrations</td>
</tr>
</tbody>
</table>
| Ideation with PPM                 | com.snc.ppm_innovation_management | Enables you to manage your demands, resources, portfolios and projects, and gives full visibility from idea to execution. Agile management and test management help you to improve productivity and service delivery. Enables you to manage ideas with full visibility from idea submission to execution. Collaborate with the idea submitter and other stakeholders to identify ideas with the greatest potential and convert them into different work entities for execution. | Inactive | true           | • com.snc.project_portfolio_suite  
• com.snc.financial_planning  
• com.snc.rate_model  
• com.snc.comments_and_feedback |
| Incident                          | com.snc.incident            | Provides base functionality for Incident Management.                                                                                                                                                       | Active   | true           | • com.snc.service  
• com.snc.incident_notification  
• com.glideapp.report.itsmincidentoverview |
| Incident Management - ATF Tests   | com.snc.incident.atf        | Delivers ATF tests for Incident Management.                                                                                                                                                                | Active   | true           |                                                                                             |
| Innovation Management Utility     | com.snc.innovation_management | Provides capability to create a work entity like demand/project from an idea.                                                                                                                                | Active   | false          |                                                                                             |
| Incident Assignment Workbench Demo| com.snc.incident_assignment | Intelligence to recommendation through dynamic matching rules/criteria.                                                                                                                                 | Inactive | true           | • com.snc.contact_management  
• com.glideapp.live_feed_document  
• com.glide.phone_number |

© 2021 ServiceNow, Inc. All rights reserved. ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Communications Management</td>
<td>com.snc.iam</td>
<td>Allows crisis managers to manage communications for major issues, to bring together all involved users via SMS, conference calls, email subscriptions, and live feed.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.assignment_workbench</td>
</tr>
<tr>
<td>Incident Management - ATF Tests</td>
<td>com.snc.incident.atf</td>
<td>Provides Incident Management ATF Tests.</td>
<td>Active</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>Incident Management - Major Incident Management</td>
<td>com.snc.incident.mim</td>
<td>Provides a recommended incident response process for managing incidents a business critical incident with pre-defined incident communication plans and a workbench to handle different aspects of the process including communication, collaboration, and postmortem.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.iam, com.snc.incident.updates, com.snc.task_outage</td>
</tr>
<tr>
<td>Incident Management Notification</td>
<td>com.snc.incident_notification</td>
<td>Provides Notification functionality to Incident Management.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Incident Overview Homepage</td>
<td>com.glideapp.report.itsm.incident_overview</td>
<td>Provides Incident Overview Homepage.</td>
<td>Active</td>
<td>false</td>
<td>com.glideapp.report</td>
</tr>
<tr>
<td>Incident Resolution Fields</td>
<td>com.snc.incident_resolution_fields</td>
<td>Adds <strong>Resolved</strong> and <strong>Resolved by</strong> fields to the Incident table, similar to <strong>Closed</strong> and <strong>Closed by</strong>, populated with a business rule when an incident is resolved or closed.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Incident Updates</td>
<td>com.snc.incident.updates</td>
<td>Incident Updates Plugin - Includes any updates to the Incident Base Plugin.</td>
<td>Active</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------</td>
<td>----</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Index Suggestion</td>
<td>com.glide.index_suggestion</td>
<td>Suggest database indexes for slow queries.</td>
<td>Active</td>
<td>false</td>
<td>Stats Tools, Column Statistics</td>
</tr>
<tr>
<td>Innovation Management</td>
<td>com.snc.innovation_management</td>
<td>Idea Management application enables idea managers to manage ideas at organization level.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.comments_and_feedback</td>
</tr>
<tr>
<td>Innovation Management - ATF Tests</td>
<td>com.snc.innovation_management</td>
<td>Innovation Management - ATF Tests provides you test cases and test suits that can be run on the Innovation Management Application.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Insert Multiple Web Service</td>
<td>com.glide.web_service_insert_multiple</td>
<td>Enables multiple inserts for the Direct SOAP API.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Instance Security Center</td>
<td>com.glide.instance_sec_center</td>
<td>This plugin activates the Instance Security Center Portal. Search for Instance Security Center in the left navigation menu.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Instance Data Replication</td>
<td>com.glide.idr</td>
<td>Replicates records from one instance to one or more other instances.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Instance Sync Connector (New in Quebec)</td>
<td>sn_instance_sync_connector</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Instance Sync Connector - Core (New in Quebec)</td>
<td>com.snc.instance_sync_connector</td>
<td>Instance Sync Connector Core plugin that provides an ability to activate and leverage Integration Hub Process Sync Framework.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.hub.process.sync</td>
</tr>
<tr>
<td>Integration - Common Components</td>
<td>com.snc.integration.common</td>
<td>Provides common scripts for integrations.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.system_import_set, com.glide.web_service_provider, com.glide.system_property_categories</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Integration - JDBC                         | com.snc.integration.jdbc | Provides integration through JDBC.                                                                                  | Inactive| false          | • com.glide.web_service_application  
|                                             |         |                                                                                                                      |         |                | • com.glideapp.agent  
|                                             |         |                                                                                                                      |         |                | • com.snc.integration.common |
|                                             |         |                                                                                                                      |         |                | • com.snc.ci.identification                                                |
|                                             |         |                                                                                                                      |         |                | • com.snc.ci.identification                                                |
| Integration - Microsoft SCCM 2016           | com.snc.integration.sccm2016 | Integration with Microsoft SCCM.                                                                                  | Inactive| false          | • com.snc.integration.jdbc  
|                                             |         |                                                                                                                      |         |                | • com.snc.ci.identification                                                |
| Integration - Multifactor Authentication    | com.snc.integration.multifactor.authentication | Set up Multifactor authentication on the instance.                                                                   | Active  | false          |                                                                             |
| Integration - Multiple Provider Single Sign-On Enhanced UI | com.snc.integration.sso.multi |                                                                              | Inactive| false          | • com.glide.ui.ng.guided_flow  
<p>|                                             |         |                                                                                                                      |         |                | • com.snc.integration.sso.multi.installer                                 |</p>
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration - Multiple Provider Single Sign-On Installer</td>
<td>com.snc.integration.sso.multi.installer</td>
<td>Use this plugin instead of the Integration - Multiple Provider Single Sign-On plugin to activate the Multiple Provider Single Sign-On feature. The multiple provider single sign-on plugin enables organizations to authenticate against multiple IDPs (Identity providers) using SAML. It also supports authentication using multiple digest configurations.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Integration - OpenID SSO (Deprecated)</td>
<td>com.snc.integration.sso.openid</td>
<td>Legacy version of single sign-on used with an external OpenID Provider (OP). OpenID Connect is provided in London but is limited to Web Services. The Single Sign-On portion is not supported at this time.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.integration.common</td>
</tr>
<tr>
<td>Integration - Tivoli Enterprise Console (TEC) 2.0</td>
<td>com.snc.integration.tivoli_tec</td>
<td>Provides version 2.0 integration with Tivoli Enterprise Console (TEC).</td>
<td>Inactive</td>
<td>false</td>
<td>• com.snc.integration.common                                                    • com.glide.web_service_application • com.glideapp.agent</td>
</tr>
<tr>
<td>Integration - Verizon eBonding</td>
<td>com.snc.integration.verizon_ebonding</td>
<td>Provides integration with Verizon eBonding.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.snc.integration.common                                                    • com.glide.custom_web_service • com.glide.static_wdsl • com.glide.custom_web_service • com.glideapp.ecc_retry_policy</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IntegrationHub Remote Process Sync License</td>
<td>com.glide.hub.remote.process.sync</td>
<td>New in Quebec</td>
<td>False</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrations - External Authentication Framework</td>
<td>com.glide.external.app</td>
<td>Inactive</td>
<td>False</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interaction Logging, Routing, and Queueing</td>
<td>com.glide.interaction</td>
<td>Interaction Logging, Routing, and Queueing.</td>
<td>Inactive</td>
<td>False</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Interactions Management</td>
<td>com.glide.interaction</td>
<td>Activates the Interactions Management System</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Interactive Analysis</td>
<td>com.glideapp.interactive_analysis</td>
<td>Interactive Analysis</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Investment Funding - ATF Tests</td>
<td>com.snc.investment_planning</td>
<td>Investment Funding - ATF Tests provides you test cases and test suits that can be run on the Investment Funding Application.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.financial_planning_pmo.atf</td>
</tr>
<tr>
<td>Investment Planning</td>
<td>com.snc.investment_planning</td>
<td>Enables continuous and flexible investment planning for the funding entities based on their priorities and strategic objectives. It provides the options of top-down and bottom-up funding and defunding an entity.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.app.grid&lt;br&gt;com.snc.app.widgets&lt;br&gt;com.snc.fiscal_calendar&lt;br&gt;com.snc.planned_task_v2</td>
</tr>
<tr>
<td>Investment Planning for PPM</td>
<td>com.snc.investment_planning</td>
<td>Enables continuous and flexible investment planning for PPM funding entities based on their priorities and strategic objectives. It provides the options of top-down and bottom-up funding and defunding an entity.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.investment_planning&lt;br&gt;com.snc.financial_planning_pmo</td>
</tr>
<tr>
<td>IP Range Based Authentication</td>
<td>com.snc.ipauthenticator</td>
<td>Controls access to an instance based on IP address.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>ISC NLU Model for Virtual Agent Conversations (New in Quebec)</td>
<td>com.glide.isc_nlu</td>
<td>Activates the Natural Language Understanding (NLU) content pack for the Instance Security Center.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.isc_virtualagent</td>
</tr>
<tr>
<td>ISC Virtual Agent Conversations (New in Quebec)</td>
<td>com.glide.isc_virtualagent</td>
<td>Activates the Virtual Agent content pack for the Instance Security Center.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.cs.chatbot, com.snc.nlu_studio</td>
</tr>
<tr>
<td>Issue Auto-Resolution (New in Quebec)</td>
<td>com.glide.cs.auto_resolution</td>
<td>Intercepts incidents submitted through the Service Portal or email and gives your end users an option to have Virtual Agent help find a resolution.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.cs.chatbot</td>
</tr>
<tr>
<td>IT Asset Management Mobile</td>
<td>com.sn_itam_mobile</td>
<td>Inventory manager can receive and create assets at the dock.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.sg, com.glide.sg.offline</td>
</tr>
<tr>
<td>ITBM Security</td>
<td>com.snc.itbm_security</td>
<td>Common plugin to manage security within IT Business Management plugins.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>IT Data Mart</td>
<td>com.snc.it_data_mart</td>
<td>Stores the information that the IT Finance application uses to allocate expenses to specific accounts and segments in the general ledger.</td>
<td>Inactive</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Item Designer support for the service catalog</td>
<td>com.glideapp.servicecatalog</td>
<td>Service Catalog item designer.</td>
<td>Active</td>
<td>true</td>
<td>com.glideapp.servicecatalog</td>
</tr>
<tr>
<td>ITOM Guided Setup</td>
<td>com.snc.guided_setup_metadata</td>
<td>ITOM Guided Setup Metadata.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.guided_setup</td>
</tr>
<tr>
<td>ITSM CSDM Best Practice - Quebec (New in Quebec)</td>
<td>com.snc.best_practice.itsm_csdm</td>
<td>ITSM CSDM Best Practices for Quebec release includes best practice configurations to support Common Service Data Model (CSDM). This plugin includes a business rule that populates the assignment group on the incident, problem, and change request based on the support group field on the CI or Service Offering.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>ITSM Guided Setup</td>
<td>com.snc.guided_setup_metadata</td>
<td>ITSM Guided Setup Metadata.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.guided_setup</td>
</tr>
<tr>
<td>ITSM Mobile</td>
<td>com.sn_itsm_mobile</td>
<td>ITSM Mobile Experience</td>
<td>Active</td>
<td>false</td>
<td>com.glide.sg</td>
</tr>
<tr>
<td>ITSM Mobile Agent</td>
<td>com.sn_itsm_mobile_agent</td>
<td>New redesigned ITSM Mobile experience for Incident Management and On-Call.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------</td>
<td>----</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
<td>--------------</td>
</tr>
<tr>
<td>ITSM NLU Model for Virtual Agent Conversations</td>
<td>com.snc.itsm.nlu</td>
<td>This plugin contains NLU models used in the Virtual Agent topics for ITSM related use cases.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.platform_ml, com.glide.dev-studio, com.snc.nlu_studio</td>
</tr>
<tr>
<td>ITSM Process Optimization Content Pack (Maintenance mode only)</td>
<td>com.sn_itsm_process_opt_cp</td>
<td>Provides pre-configured process optimization models and improvement initiatives for the ITSM Processes.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>ITSM Roles - Change Management</td>
<td>com.snc.itsm.roles.change_management</td>
<td>This plugin is included with the ITSM Roles plugin. This plugin adds the sn_change_read and sn_change_write roles. It also updates the existing security model for Change Management to factor these new roles.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>ITSM Roles - Incident Management</td>
<td>com.snc.itsm.roles.incident_management</td>
<td>This plugin is included with the ITSM Roles plugin. This plugin adds the sn_incident_read and sn_incident_write roles. It also updates the existing security model for Incident Management to factor these new roles.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>ITSM Roles - Problem Management</td>
<td>com.snc.itsm.roles.problem_management</td>
<td>This plugin is loaded with the ITSM Roles plugin.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>ITSM Roles - Request Management</td>
<td>com.snc.itsm.roles.request_management</td>
<td>This plugin adds sn_request_read and sn_request_write. It also updates the existing security model for Request Management to factor these new roles.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>ITSM Shared VA Topic Blocks</td>
<td>com.glideapp.cs.itsm_topic_blocks</td>
<td>This plugin contains prebuilt re-usable conversation topic blocks for common actions like ordering from the catalog and searching the knowledge base.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITSM Spoke</td>
<td>com.snc.itsm.spoke</td>
<td>This Spoke enables Flow Designers to automate and create flows and actions associated with ITSM</td>
<td>Active</td>
<td>false</td>
<td>com.glide.hub</td>
</tr>
<tr>
<td>ITSM Virtual Agent Conversations</td>
<td>com.snc.itsm.virtualagent</td>
<td>This plugin contains prebuilt conversation topics for ITSM related use cases.</td>
<td>Active</td>
<td>true</td>
<td>• com.glide.cs.chatbot</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.service-portal</td>
</tr>
<tr>
<td>ITSM Virtual Agent Conversation Topics Lite (Maintenance mode)</td>
<td>com.snc.itsm.virtualagent_lite</td>
<td>Read only conversations for basic ITSM self service use cases, including opening incidents, checking status, searching the knowledge base, submitting requests, and checking for outages.</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.cs.chatbot_lite</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glideapp.cs.sm_topic_blocks</td>
</tr>
<tr>
<td>ITSM Workspace</td>
<td>com.snc.agent_workspace.itsm</td>
<td>The ITSM Workspace plugin provides you the functionality of ITSM Agent Workspace. The plugin is available by default for new and existing users. The ITSM Workspace plugin also activates the ITSM Workspace Landing Pages (com.snc.agent_workspace.itsm.landing_page) plugin.</td>
<td>Active</td>
<td>false</td>
<td>• com.agent_workspace</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glideapp.servicecatalog.workspace</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.agent_recommend</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.agent_workspace.itsm.landing_page</td>
</tr>
<tr>
<td>ITSM Workspace Landing Pages</td>
<td>com.snc.agent_workspace.itsm_landing_page</td>
<td>Deleting ITSM Agent Workspace Landing Pages - basic version.</td>
<td>Inactive</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>--------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------</td>
<td>---------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>JDBC Step for ServiceNow IntegrationHub</td>
<td>com.glide.hub.action_step.jdbc</td>
<td>Activates the JDBC step in Flow Designer, enabling you to create a reusable action to send SQL commands to a relational database.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.hub.action_step.template</td>
</tr>
<tr>
<td>JS Code Coverage Debug</td>
<td>com.glide.js.coverage</td>
<td>Debug utility that collects coverage data for server-side Javascript.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.glide.sessiondebug</td>
</tr>
<tr>
<td>JSDebugger</td>
<td>com.glide.glide-js-debugger</td>
<td>ServiceNow server-side scripts debugger.</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.glide-js-debugger-api</td>
</tr>
<tr>
<td>JSON Service request/response model</td>
<td>com.snc.application.json_service</td>
<td>Core components and helpers for a JSON request/response model. Includes JSON and XML transports for NG and GlideAjax support. An extension of the processor framework.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>KCS Integration for Incident Management</td>
<td>com.snc.incident.knowledge</td>
<td>Provides integration of Incident Management with the Advanced Knowledge Management features.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.knowledge_advanced.installer</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>-----------------------------------------------</td>
</tr>
</tbody>
</table>
| Keylines Business Service Maps  | com.snc.keylines_bsm_map| An interactive and graphical interface to visualize Configuration Items (CIs) and their relationships. Provides filtering capabilities to manage data being displayed, allowing for configuration by the user to view in context to their role. Additional capabilities provide for the displaying of related tasks such as Incidents, Problems, Changes and Certification Tasks. | Active| false          | • com.glide.diagrammer  
• com.glideapp.bsm_map2 |
<p>| Knowledge API                   | sn_km_api               | Provides the ability to search, view, and fetch most-viewed and featured knowledge articles.                                                                                                                  | Inactive| false          |                                               |
| Knowledge Blocks                | com.snc.knowledge_blocks| This plugin adds an advanced editing feature to Knowledge Management which allows user to create re-usable content blocks that can be included in existing knowledge articles. This feature will give the ability to have one large article and be able to just display pieces of that article to specific users. | Active| true           | com.snc.knowledge_advanced.installer          |
| Knowledge Capabilities in UI Builder (New in Quebec) | com.snc.uib.knowledge | Enables configurable Knowledge Management artifacts (Pages, Data transforms, and GraphQL queries) in UI Builder.                                                                                             | Active| false          |                                               |</p>
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
</table>
| Knowledge Management Core                  | com.glideapp.knowledge | Installs the core Knowledge Management items used to allow other Knowledge related plugins to work, such as Knowledge V3, Knowledge Advanced, Knowledge Service Portal. This plugin is activated by default. | Active | true           | • com.glide.ui.angular  
• com.glide.ui.ng  
• com.glideapp.user_criteria  
• com.snc.db.rotation  
• com.glideapp.live_feed_v2  
• com.glideapp.report.knowledge.overview |
| Knowledge Document                         | com.snc.knowledge_document | Adds knowledge-based functionalities to the Managed Documents plugin. You can create a knowledge article from a document, or update a knowledge document to a newer revision. | Inactive | false          | com.snc.document_management                                                  |
| Knowledge Management - External Content Integration | com.snc.knowledge.external_integration | Adds external content search capabilities to the knowledge management application. Once configured, this feature creates a copy of the external content on ServiceNow as knowledge articles, and then indexes the articles through Zing Search. You must have appropriate reuse and copy privileges before you configure an external source to be searchable using this feature. | Inactive | true           | • com.snc.core.automation.connection_credential  
• com.snc.knowledge3  
• com.snc.knowledge_advanced.installer |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge Management - Mobile Requestor</td>
<td>com.glideapp.knowledge.mobile_requestor</td>
<td>This is a maintenance plugin used to activate Knowledge Management Mobile Requestor features.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.glideapp.knowledge</td>
</tr>
<tr>
<td>Knowledge Management - Service portal</td>
<td>com.snc.knowledge_serviceportal</td>
<td>Provides knowledge management features on the service portal.</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.service-portal.esm</td>
</tr>
<tr>
<td>Knowledge Management Advanced</td>
<td>com.snc.knowledge_advanced</td>
<td>This plugin adds advanced features to Knowledge Management such as version control and subscriptions. It requires that all Knowledge bases are Knowledge v3. Please use Knowledge Management Advanced Installer plugin to activate.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.knowledge3</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>---------------------------------------------------</td>
</tr>
</tbody>
</table>
| Knowledge Management Advanced Installer         | com.snc.knowledge_advanced.installer | Use this plugin to install the Knowledge Advanced plugin. When you activate/upgrade this plugin, it will do validations on knowledge articles and knowledge bases to make sure that the Knowledge Advanced plugin can be successfully installed. If validation fails, look at the errors in the Plugin Activation Logs and follow instructions given to fix them. Once all the issues are fixed, please re-run this plugin to install Knowledge Advanced. | Inactive | false          | - com.glide.ui.angular  
- com.glide.ui.ng  
- com.glideapp.knowledge2  
- com.glideapp.user_criteria  
- com.snc.contextual_search  
- com.snc.db.rotation  
- com.glideapp.live_feed_v2  
- com.glideapp.report.knowledge.overview |
| Knowledge Management V3                         | com.snc.knowledge3  | Activate this plugin when you upgrade from Eureka or earlier.                               | Active | true           | - com.glide.ui.angular  
- com.glide.ui.ng  
- com.glideapp.knowledge2  
- com.glideapp.user_criteria  
- com.snc.contextual_search  
- com.snc.db.rotation  
- com.glideapp.live_feed_v2  
- com.glideapp.report.knowledge.overview |
| Knowledge Management Wiki Support               | com.glideapp.knowledge2.wiki | Activate this plugin to enable support for Wiki type Knowledge articles.                   | Active | false          | - com.glide.wiki  
- com.glideapp.knowledge2 |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge Management KCS Capabilities plugin</td>
<td>com.snc.knowledge_kcs_capabilities</td>
<td>Activate this plugin to enable the use of KCS roles (kcs_contributor, kcs_publisher, and kcs_candidate) and use the metadata fields for the KCS article state (governance and confidence).</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Knowledge Product Entitlements</td>
<td>com.snc.kb_product_entitlements</td>
<td>Knowledge Product entitlements, enables Customer Service admins to restrict access to customers based on products they are entitled to.</td>
<td>Inactive</td>
<td>false</td>
<td>com.sn_customerservice</td>
</tr>
<tr>
<td>Knowledge Management - Add-in for Microsoft Word</td>
<td>com.snc.knowledge.ms_word</td>
<td>Enables authoring content in Microsoft Word and publishing it as a knowledge article using a Word add-in.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.servicenow_now_kb_office_addin</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glideapp.knowledge</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.sn_outlook_addin</td>
</tr>
<tr>
<td>KPI Composer</td>
<td>sn_kpi_composer</td>
<td>KPI Composer is an application for designing KPIs and Dashboards by using performance measurement methodologies.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>KPI Details Workspace Integration</td>
<td>com.snc.pa.kpi_details_ws_int</td>
<td>Performance Analytics - KPI Details allows user to explore more for a certain KPI, this plugin used to integrate sn-kpi-details component to workspace.</td>
<td>Active</td>
<td>false</td>
<td>• com.agent_workspace</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.workspace_core</td>
</tr>
<tr>
<td>LDAP Support Enhanced UI</td>
<td>com.glide.ldap.ui</td>
<td></td>
<td>Inactive</td>
<td>false</td>
<td>• com.glide.ui.ng.guided_flow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.ldap</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Legal Request Management</td>
<td>sn_lg_ops</td>
<td>Create and manage legal requests for legal teams. Includes workspace.</td>
<td>Active</td>
<td>true</td>
<td>• com.workspace_core</td>
</tr>
<tr>
<td>(Available in the ServiceNow Store)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.ui.checklist</td>
</tr>
<tr>
<td>Legal Matter Management</td>
<td>sn_lg_matter</td>
<td>Create and manage legal matter projects. Includes workspace.</td>
<td>Active</td>
<td>true</td>
<td>sn_lg_ops</td>
</tr>
<tr>
<td>(Available in the ServiceNow Store)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legal: Counsel Center</td>
<td>sn_lg_workspace</td>
<td>Manage and resolve legal requests and matters.</td>
<td>Active</td>
<td>false</td>
<td>sn_lg_ops</td>
</tr>
<tr>
<td>(Available in the ServiceNow Store)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legal: Counsel Center Components</td>
<td>sn_lg_ws_comps</td>
<td>Includes components developed in Now Experience UI Framework and used in Legal Counsel Center.</td>
<td>Active</td>
<td>false</td>
<td>sn_lg_ops</td>
</tr>
<tr>
<td>(Available in the ServiceNow Store)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legal: Mobile</td>
<td>sn_lg_mobile</td>
<td>Mobile experience for Legal applications.</td>
<td>Active</td>
<td>false</td>
<td>sn_lg_ops</td>
</tr>
<tr>
<td>(Available in the ServiceNow Store)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legal Virtual Agent Conversations</td>
<td>sn_lg_va</td>
<td>Contains pre-built template conversation topics for Legal Service Delivery.</td>
<td>Active</td>
<td>false</td>
<td>• sn_lg_ops</td>
</tr>
<tr>
<td>(Available in the ServiceNow Store)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.cs.chatbot</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Legal Service Management (Maintenance mode only) Planned for deprecation after Feb 1, 2023</td>
<td>com.snc.legal_service_automation</td>
<td>Manages legal matters and enables users to report and track matters. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.service_management.core</td>
</tr>
<tr>
<td>Legal Service Management Mobile</td>
<td>com.snc.legal_service_automation</td>
<td>Manages Legal Service Management mobile components.</td>
<td>Inactive</td>
<td>true</td>
<td>• com.snc.legal_service_automation</td>
</tr>
<tr>
<td>Limit Concurrent Sessions</td>
<td>com.glide.limit.concurrent.sessions</td>
<td>Activate this plugin to limit concurrent interactive sessions on the instance.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Link Generator</td>
<td>com.snc.linkgenerator</td>
<td>Activates the Link Generator that allows you to create deep links on an HR form to access information outside the application. You can generate URLs to manage content, knowledge articles, and catalogs or access social media or fulfillment requests</td>
<td>Inactive</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>List v2</td>
<td>com.glide.list_v2</td>
<td>Updates to the display of lists that include a cleanup UI, hierarchical lists, and related lists embedded in forms.</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.tiny_url</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.ui_list_edit_with_form</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.db_context_menu</td>
</tr>
<tr>
<td>List v3 Components</td>
<td>com.glide.ui.list_v3_components</td>
<td>Provides components required for List v3, including REST endpoints and Angular components.</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.ui.list_api</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.ui.ng</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.ui.ng.amb</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.ui.ng.form_elements</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.ui.ng.filter</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glideapp.report.charting_v2</td>
</tr>
<tr>
<td>Live Agent Conversation Settings</td>
<td>com.glide.cs.live_agent_settings</td>
<td>Live Agent Conversation Settings</td>
<td>Active</td>
<td>false</td>
<td>com.glide.interaction</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
</table>
| Live Feed                                  | com.glideapp.live_feed_v2 | Provides an updated application to post and share content in a ServiceNow instance. | Active | true           | • com.glideapp.live_feed
|                                             |                           |                                                                               |       |                | • com.glideapp.ui_components                                                  |
| Live Feed                                  | com.glideapp.live_feed    | Provides a place to post and share content in a ServiceNow instance.           | Active | true           | • com.glide.custom_web_service
|                                             |                           |                                                                               |       |                | • com.glideapp.live_common
|                                             |                           |                                                                               |       |                | • com.glide.notification                                                     |
| Live Feed Document - follow tasks (Incident, Change, etc.) | com.glideapp.live_feed_document | Enables you to manage your task conversations and comments from My Feed or a document group. | Active | false          | com.glideapp.live_feed                                                     |
| Localization Framework (New in Quebec)      | com.glide.localization_framework | A framework to manage localization workflows across the platform and products. To activate this plugin, install the Localization Framework Installer plugin. | Active | false          | • com.glide.localization_framework.sdl_spoke
|                                             |                           |                                                                               |       |                | • com.glide.localization_framework.xtm_spoke
|                                             |                           |                                                                               |       |                | • com.glide.localization_framework.va
|                                             |                           |                                                                               |       |                | • com.glide.localization_framework.service_catalog
<p>|                                             |                           |                                                                               |       |                | • com.glide.i18n                                                           |</p>
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Localization Framework Installer</td>
<td>com.glide.localization_frameworkinstaller</td>
<td>Enhances the existing experience of translating the artifacts in an instance by automating most of the manual tasks in the localization process.</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.hub.integrations&lt;br&gt;• com.glide.localization_framework&lt;br&gt;• com.glide.localization_framework.sdl_spoke&lt;br&gt;• com.glide.localization_framework.xtm_spoke&lt;br&gt;• com.glide.localization_framework.va&lt;br&gt;• com.glide.localization_framework.service_catalog</td>
</tr>
<tr>
<td>Macroponent Catalog Item for UIB (New in Quebec)</td>
<td>com.glideapp.servicecatalog.macroponent</td>
<td>Component for Now Experience Builder for Catalog Item and Record Producer.</td>
<td>false</td>
<td>• com.glideapp.servicecatalog.macroponent&lt;br&gt;• com.glideapp.servicecatalog.form&lt;br&gt;• com.glideapp.servicecatalog.action&lt;br&gt;• com.glideapp.servicecatalog.description&lt;br&gt;• com.glideapp.servicecatalog.form_connected&lt;br&gt;• com.glideapp.servicecatalog.price&lt;br&gt;• com.glideapp.servicecatalog.quantity&lt;br&gt;• com.glideapp.servicecatalog.additional_details&lt;br&gt;• com.glideapp.servicecatalog.request_for</td>
<td></td>
</tr>
<tr>
<td>Magellan Navigator</td>
<td>com.glide.ui.magellan_navigator</td>
<td>Provides a redesigned application navigator for UI16. Combines standard navigation capabilities, customizable favorites, and recently accessed items in a single responsive control.</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.ui.magellan_navigator_api&lt;br&gt;• com.glide.ui.doctype&lt;br&gt;• com.glide.ui.ng</td>
</tr>
<tr>
<td>Maintenance Schedules</td>
<td>com.snc.maintenance_schedules</td>
<td>Links configuration items to maintenance schedules. The maintenance schedules are checked against the planned dates for changes, and those that appear outside the maintenance schedule are so marked.</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.schedules&lt;br&gt;• com.snc.cmdb</td>
</tr>
<tr>
<td>Major Issue Management</td>
<td>com.sn_majorissue_mgtdyn</td>
<td>A set of capabilities used to manage customer-facing communications and resolution processes for common issues.</td>
<td>Inactive</td>
<td>true</td>
<td>• com.sn_customerservice&lt;br&gt;• com.sn_publications&lt;br&gt;• com.snc.task_communication_management</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------------------</td>
<td>----------------------------------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>Managed documents</td>
<td>com.snc.document_management</td>
<td>Lightweight ITIL-based solution for managing electronic documents within your ServiceNow instance. To enable the ability to publish to the knowledge base, activate the Knowledge Document plugin.</td>
<td>Inactive</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>Manager Workspace (Maintenance mode only)</td>
<td>com.snc.manager_workspace</td>
<td>Manager Workspace App core shell. Install ITSM Manager workspace or CSM Manager workspace to get the modules</td>
<td>Active</td>
<td>true</td>
<td>com.snc.wfo</td>
</tr>
<tr>
<td>Marketing Service Management (Maintenance mode only) Planned for deprecation after Feb 1, 2023</td>
<td>com.snc.marketing_service_automation</td>
<td>Manages marketing requests and enables users to report and track those requests. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.service_management.core</td>
</tr>
<tr>
<td>Merge Tool</td>
<td>com.glide.ui.mergetool</td>
<td>User interface for performing merges between two payloads.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.ui.angular, com.glide.snc_code_editor</td>
</tr>
<tr>
<td>Metadata Source Control</td>
<td>com.glide.source_control</td>
<td>Source control integration applies and commits changes in an external repository.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.system_update_set</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Metadata Tree</td>
<td>com.snc.metadata_tree</td>
<td>Hierarchical representation of metadata.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.apps_file</td>
</tr>
<tr>
<td>Metadefender Integration</td>
<td>com.snc.threat.metadefender</td>
<td>Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.threat.intelligence</td>
</tr>
<tr>
<td>Metric Definition</td>
<td>com.glide.metrics</td>
<td>Provides an easy, declarative way to define metrics and allows the definitions to be tracked and stored by the system.</td>
<td>Active</td>
<td>true</td>
<td>com.glide.schedules</td>
</tr>
<tr>
<td>MetricBase</td>
<td>com.snc.clotho</td>
<td>Time-series data storage and processing.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.glide.highcharts</td>
</tr>
<tr>
<td>MetricBase Demo</td>
<td>com.snc.clotho.demo</td>
<td>Sample time-series data you can use to explore MetricBase functionality.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.clotho</td>
</tr>
<tr>
<td>Microsoft AD Spoke for IntegrationHub</td>
<td>com.sn.ad.spoke</td>
<td>The AD Spoke for IntegrationHub provides actions that a Process Analyst can use when designing flows. The actions allow them to automate the management of users, groups, computers, and objects in AD.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.glide.hub.designer_backend.model</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.hub.action_step.powershell</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------</td>
<td>----</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
<td>--------------</td>
</tr>
</tbody>
</table>
| Microsoft Azure AD Spoke for IntegrationHub | com.sn.azure_ad.spoke | The Azure AD Spoke for IntegrationHub provides actions that a Process Analyst can use when designing flows. The actions allow them to automate the management of users, security groups, and office groups. User management includes applying licenses that result in user provisioning into Office 365. | Inactive | false | • com.glide.hub.designer_backend.model
 • com.glide.hub.action_steps.rest |
| Microsoft Azure AD Spoke for Password Reset | com.sn.password_reset.aad.spoke | The Password Reset Azure AD Scoped App provides a prebuilt connection to credential stores in Azure AD, allowing reset and changing of password. | Active | false | • com.sn.azure_ad.spoke
 • com.glideapp.password_reset
 • com.sn.password_reset.auth |
| Microsoft Azure Translation Spoke | com.glide.microsoft_translation_spoke | Using Microsoft translation services, adds ability to translate text from one language to another and detect the language of text. | Inactive | false | com.glide.hub.integrations |
| Microsoft OneDrive document services Spoke | com.sn.documents.onedrive | Collaborate in Microsoft OneDrive and perform copy, delete, restore, and version actions on documents directly in a ServiceNow instance. This integration is bi-directional: Changes are reflected in both Microsoft OneDrive and in the instance. | Active | false | • com.sn.onedrive.spoke
 • com.sn.azure_ad.spoke |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft OneDrive Spoke</td>
<td>com.sn.onedrive.spoke</td>
<td>Contains data model needed to integrate with third-party document service providers.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>MID Server</td>
<td>com.glideapp.agent</td>
<td>The Management, Instrumentation, and Discovery (MID) Server is a Java application that runs as a Windows service or UNIX daemon. The MID Server facilitates communication and movement of data between the ServiceNow platform and external applications, data sources, and services.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.custom_web_service</td>
</tr>
<tr>
<td>MID Server Distributed Cluster</td>
<td>com.snc.agent.distributed.cluster</td>
<td>Enables the MID Server distributed cluster type, for Operational Intelligence.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.sa.metric</td>
</tr>
<tr>
<td>MID Server Key Management Framework Signature Configuration (New in Quebec)</td>
<td>com.glideapp.agent.kmf_config</td>
<td>Creates KMF signature configuration records for MID Server tables.</td>
<td>false</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Mobile Analytics</td>
<td>com.glide.mobile.analytics</td>
<td>Checks for new mobile applications to register, syncs Mobile Analytics instance settings to the ServiceNow server, and provides users access to the Mobile Analytics Dashboard. This plugin adds the mobile_analytics_admin and mobile_analytics_viewer roles.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.serviceproxy</td>
</tr>
<tr>
<td>Mobile Card Builder (New in Quebec)</td>
<td>com.sn_mobile_studio_itemview_builder</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile Employee My Assets</td>
<td>com.glide.mobile-employee.myassets</td>
<td>This plugin contains the configuration and records to create the my assets view that are used in Mobile Employee Experience native application. Do not activate this plugin directly. Activating com.glide.mobile-employee will activate this plugin for you.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Mobile Device ITIL and Service Management</td>
<td>com.snc.itil_mobile</td>
<td>Applications and modules for ITIL and Service Management.</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.labels</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.mobile</td>
</tr>
<tr>
<td>Mobile Studio</td>
<td>com.glide.sg-studio</td>
<td>Plugin for Mobile Studio</td>
<td>Active</td>
<td>false</td>
<td>com.glide.sg</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Mobile UI</td>
<td>com.glide.ui.m</td>
<td>User interface for mobile devices running iOS 6+ or Android 4+ with the Chrome browser. Provides nearly full-product functionality. Adds a System Mobile UI application to the application navigator in the standard UI for configuring the mobile UI.</td>
<td>Active</td>
<td>true</td>
<td>• com.glide.wiki&lt;br&gt; • com.glide.labels&lt;br&gt; • com.glide.db_images&lt;br&gt; • com.glide.ui.font_icons&lt;br&gt; • com.glide.ui.ng&lt;br&gt; • com.glide.ui.zerpo&lt;br&gt; • com.glide.ui.tablet.theme&lt;br&gt; • com.glide.ui.recent_selections&lt;br&gt; • com.glide.ui.table_titles&lt;br&gt; • com.snc.platform.security.oauth&lt;br&gt; • com.glide.ui.magellan_navigator_api&lt;br&gt; • com.glide.ui.list_api&lt;br&gt; • com.glide.notification.push</td>
</tr>
<tr>
<td>Mobile Publishing</td>
<td>com.glide.sn-mobile-whitelabel</td>
<td>Mobilew plugin to handle custom app branding requests, statuses, and publishing.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Model Management</td>
<td>com.snc.model</td>
<td>Enables you to manage and maintain model categories, models, suites, and bundled models.</td>
<td>Active</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>Mutex stats</td>
<td>com.glide.stats.mutex</td>
<td>Mutex stats.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.stats</td>
</tr>
<tr>
<td>My Assets</td>
<td>com.snc.asset_myassets</td>
<td>Provides users with self-service access to their own assets, contracts, and requests.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.asset_management</td>
</tr>
<tr>
<td>Name-Value Pairs field editor</td>
<td>com.glide.ui.name_values_editor</td>
<td>Adds a detailed editor for name-value pairs field types.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.ui.ng</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Natural Language Query</td>
<td>com.snc.nlq</td>
<td>Enables you to activate the Natural Language Query (NLQ) service in ServiceNow UI. NLQ translates natural language utterances into glide queries and retrieves information from Glide DB. Beginning in Quebec, this capability is exposed through the Analytics Center in Agent Workspace.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.platform_ml</td>
</tr>
<tr>
<td>Next-Gen BSM</td>
<td>com.snc.ng_bsm</td>
<td>Next Generation BSM (NG-BSM) built on D3 and Angular. Provides an enhanced, modern interactive graphical interface to visualize Configuration Items (CIs) and their relationships. Provides filtering capabilities to manage data being displayed and displays related information for CIs such as Events, Incidents, Problems, and Changes.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.ui.heisenberg</td>
</tr>
<tr>
<td>NG Common for the Guided Flow experience</td>
<td>com.glide.ui.ng.guided_flow</td>
<td>Common Angular Components for the Guided Flow experience.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.glide.ui.tablet.theme           • com.glide.ui.ng           • com.glide.ui.themes.doctype</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>NG shared components</td>
<td>com.glide.ui.ng</td>
<td>Provides libraries and services common to plugins using Angular.</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.ui.angular</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.ui.angularui</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.ui.ng.amb</td>
</tr>
<tr>
<td>NLU Common Model</td>
<td>com.glide.nlu.model</td>
<td>The NLU Common Model plugin packages commonly used pattern entities that can be imported and used in any NLU model in the NLU Model Builder. Commonly used patterns like email, phone and ServiceNow specific pattern entities like INT, RITM are made available.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.nlu</td>
</tr>
<tr>
<td>NLU Model Builder</td>
<td>com.snc.nlu_studio</td>
<td>Enables the creation of Natural Language Understanding (NLU) models. These models can understand the intent (action) and entities (details about the action) for a given user utterance/sentence.</td>
<td>Active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NLU Model Builder - Core</td>
<td>com.glide.nlu</td>
<td>Core NLU. Installs the required tables for persisting NLU models that are created using the NLU Model Builder.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Normalization Data Services Client</td>
<td>com.glide.data_services_canonicalization.client</td>
<td>Helps maintain consistency by ensuring that records for a given company refer to that company by the same name.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.cmdb</td>
</tr>
<tr>
<td>Normalization Data Services Configuration</td>
<td>com.glide.data_services_canonicalization.config</td>
<td></td>
<td></td>
<td></td>
<td>com.snc.guided_setup</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Notification Preference Service</td>
<td>com.glide.notification.preference</td>
<td>Defines javascript and REST API for configuring notification preferences.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.notification</td>
</tr>
<tr>
<td>Notification Preference User Interface</td>
<td>com.glide.notification.preference</td>
<td>Defines the user interface for the Notifications tab in the system settings menu.</td>
<td>Active</td>
<td>false</td>
<td>NG shared components, com.glide.notification.subscription, Notification System Push Addon, com.glide.notification.preference.service</td>
</tr>
</tbody>
</table>
| Notification System Push Addon  | com.glide.notification.push | Adds support for push notifications to the notification system.              | Active  | false          | • com.glide.notification  
|                                 |                     |                                                                             |         |                | • com.glide.push                                    |
| Notify                          | com.snc.notify      | Provides powerful platform features for workflow-driven voice calls, conference calls, and SMS messages making it possible to create flexible Interactive Voice Response (IVR) systems to do virtually anything. Requires the Twilio Driver and a separate contract with Twilio for SMS and Voice capabilities. | Inactive| true           | • com.glide.phone_number  
|                                 |                     |                                                                             |         |                | • com.snc.notify.twilio                                   |
| Notify-Twilio Direct driver    | com.snc.notify.twilio_direct | Provides Notify support for Twilio. Requires a separate contract with Twilio for SMS/Voice capabilities. | Inactive| false          | • com.snc.sn_context  
<p>|                                 |                     |                                                                             |         |                | • com.snc.notify                                                   |</p>
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Now Platform Encryption (New in Quebec)</td>
<td>com.glide.now.platform.encryption</td>
<td>NOW Platform Encryption (NPE) enables field encryption with NIST best practice Key Management Framework (KMF) key lifecycle management and FIPS 140-2-I3 HSM key protection along with the automating Key and Data Migration jobs.</td>
<td>false</td>
<td>false</td>
<td>• com.glide.kmf.global • com.glide.encryption</td>
</tr>
<tr>
<td>OAuth 2.0</td>
<td>com.snc.platform.security.oauth</td>
<td>The implementation of OAuth 2.0 to support token granting and authentication.</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.certificates • com.snc.platform.security.oauth.legacy</td>
</tr>
<tr>
<td>OAuth 2.0 legacy (Do not activate. Use ‘OAuth 2.0’)</td>
<td>com.snc.platform.security.oauth.legacy</td>
<td>implementation of OAuth 2.0. Install com.snc.platform.security.oauth instead.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>ODBC Commons</td>
<td>com.glide.odbc.commons</td>
<td>ODBC Commons.</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.script.vtable • com.snc.on_call_rotation</td>
</tr>
<tr>
<td>On-Call: PA and Reports Content Pack</td>
<td>com.snc.on_call.par.content</td>
<td>• Dashboards • Reports and Performance Analytics content pack for On-Call Schedules and Escalations</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.script.vtable • com.snc.on_call_rotation</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>On-Call Scheduling</td>
<td>com.snc.on_call_rotation</td>
<td>Provides the ability to create on-call schedules and escalation trees. When an incident is created, dynamically route the escalation to an on-call resource. On Call allows you to configure and build different on-call schedules per process and assignment group. When utilizing the Notify plugin, resources can use SMS and Voice escalations to interact with the escalation to acknowledge incidents, and so on.</td>
<td>Inactive</td>
<td>true</td>
<td>• com.glide.schedules</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.notification</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.ui.ng</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.app.calendar</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.fullcalendar</td>
</tr>
<tr>
<td>Openframe</td>
<td>com.sn_openframe</td>
<td>An interface to integrate external communication systems with ServiceNow. This plugin brings a UI frame that is accessible and available anywhere within ServiceNow screens.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.ui.ng</td>
</tr>
<tr>
<td>Openframe Integration App</td>
<td>com.sn_openframe_integration</td>
<td>Holds records to support UIB framework.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>(New in Quebec)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Operational Intelligence</td>
<td>com.snc.sa.metric</td>
<td>Operational Intelligence provides the ability to capture, and then explore and analyze operational metrics data, identifying and indicating anomalies.</td>
<td>Active</td>
<td>false</td>
<td>• com.glideapp.itom.snac</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.sa.mid.webserver</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.clotho</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.highcharts</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.agent.distributed.cluster</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.ui.list_v3_components</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.itom.ui</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.sa.metric.health</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.oi-scoped-app,</td>
</tr>
<tr>
<td>Operational Intelligence - WS Scoped App</td>
<td>com.oi-scoped-app</td>
<td>Operational Intelligence - Workspace Scoped App for different user interfaces.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.graphq</td>
</tr>
<tr>
<td>Ordered Email Processing</td>
<td>com.glide.email_ordered_processing</td>
<td>Allows inbound email actions to be ordered, and programmatically stop processing.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Organization Extension</td>
<td>com.snc.organization_extension</td>
<td>Provides Goals, Enterprise Strategy and Business Unit strategy entities.</td>
<td>Active</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>Organization Management</td>
<td>com.snc.organization_management</td>
<td></td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Outage Numbering</td>
<td>com.snc.outage_numbering</td>
<td>This plugin will introduce a new unique identifier column for the outage table. This plugin is activated automatically for all instances except those who already have a number prefix column on the outage table. Please do not activate this plugin if you have a number prefix for this table.</td>
<td>Active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Outbound Email Notifications</td>
<td>com.glide.email_outbound</td>
<td>Enables outbound email notifications.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Outbound HTTP Log</td>
<td>com.glide.outbound_http_log</td>
<td>Outbound HTTP request log</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Outbound Tracking</td>
<td>com.glide.outbound_tracking</td>
<td>Outbound request tracking.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.usageanalytics</td>
</tr>
<tr>
<td>Outlook Actionable Messages</td>
<td>com.sn_ms_oam</td>
<td>Outlook Actionable Messages</td>
<td>Active</td>
<td>false</td>
<td>com.snc.platform.security.oauth</td>
</tr>
<tr>
<td>Outsourced Customer Service (Maintenance mode only)</td>
<td>com.snc.outsourced_service_organisation</td>
<td>Outsourced Service Provider (OSP) organizations. An enterprise can engage OSPs to provide customer service to external customers for reasons such as regional support, different languages, seasonal availability and so on.</td>
<td>Active</td>
<td>false</td>
<td>• com.sn_customerservice</td>
</tr>
<tr>
<td>Overview Pages</td>
<td>com.glide.ui.overview_help</td>
<td>Framework for Overview pages.</td>
<td>Active</td>
<td>false</td>
<td>• com.snc.outsourced_service_provider</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Packages Call Removal Tool</td>
<td>com.glide.script.packages_call_removal</td>
<td>Scans scripts for Packages calls to ServiceNow Java classes, proposes changes to replace them with alternate scriptable names, and facilitates the script changes. Packages calls to ServiceNow Java classes will eventually be disallowed in a future ServiceNow release, and this utility helps prepare an instance for that.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>PA Dashboard for NLU Model Builder</td>
<td>com.glide.nlu.pa</td>
<td>The NLU Model Builder PA plugin tracks the performance of NLU models being used in Virtual Agent. The plugin packages an NLU Performance dashboard which reports on how many predictions were correct, how many predictions were skipped by the NLU model and how many were considered wrong by Virtual Agent users.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Password Reset                        | com.glideapp.password_reset | Provides the ability to create self-service and service desk password reset processes for a ServiceNow instance.                                                                                           | Active | true           | • com.snc.process_flow_formatter  
|                                       |                        |  
|                                       |                        | • com.glide.notification  
<p>|                                       |                        | • com.glide.usageanalytics |</p>
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Reset - Orchestration Add-on</td>
<td>com.glideapp.password_reset_orchestration</td>
<td>Provides an add-on to enable the use of ServiceNow Orchestration. Includes support for Active Directory and remote SOAP based credential systems.</td>
<td>Inactive</td>
<td></td>
<td>Password Reset, Orchestration</td>
</tr>
<tr>
<td>Password Reset Spoke</td>
<td>com.sn.password_reset.ah</td>
<td>Provides subflows and actions in IntegrationHub required for the Password Reset application.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.hub.designer_backend.model</td>
</tr>
<tr>
<td>Password Reset Windows App</td>
<td>com.glideapp.password_reset_windows</td>
<td>Password Reset Windows integration.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Payment Operations (New in Quebec)</td>
<td>com.sn_bom_payment</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PDF Generator</td>
<td>com.snc.pdf_generator</td>
<td>Provides a tool to generate PDF documents. The Human Resources application uses this with various documents.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.signaturepad</td>
</tr>
<tr>
<td>Performance Analytics</td>
<td>com.snc.pa</td>
<td>Enables users to define and track key performance indicators (KPIs) and visualize these in scorecards and dashboards. Users can report and compare multiple time series, do advanced trend analysis, and compare their performance with preset targets.</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.ui.angular</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glideapp.report</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glideapp.home.publishers</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.core.automation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.usageanalytics</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>Performance Analytics - Administrator Console</td>
<td>com.snc.pa.administration.com</td>
<td>A single console where you can:</td>
<td>Active</td>
<td>false</td>
<td>com.snc.pa</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Explore and manage Performance Analytics widgets and dashboards, including</td>
<td></td>
<td></td>
<td>com.glide.ui.ng</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Diagnose and resolve configuration errors</td>
<td></td>
<td></td>
<td>com.glide.ui.ng.amb</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• View usage analytics</td>
<td></td>
<td></td>
<td>com.snc.pa.diagnostics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Modify advanced configuration settings</td>
<td></td>
<td></td>
<td>com.snc.pa.usage.overview</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Access ServiceNow help.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Performance Analytics - Configuration Generator</td>
<td>com.snc.pa.configurationgenerator</td>
<td>Provides a configuration generator for creating a set of Performance Analytics indicators, breakdowns, dashboards, and widgets based on the task-derived table.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.pa</td>
</tr>
<tr>
<td>Performance Analytics - GRC: Advanced Dashboards</td>
<td>com.sn_grc_pa_advanced</td>
<td>Contains the Advanced Performance Analytics dashboards created for GRC.</td>
<td>Inactive</td>
<td>true</td>
<td>com.sn_compliance</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>com.sn_risk_advanced</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>com.sn_audit</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
<td>-----------------------------------</td>
</tr>
</tbody>
</table>
| Performance Analytics - Content Pack - Advanced Work Assignment | com.snc.pa.awa    | Provides Performance Analytics indicators and visualizations for Advanced Work Assignment. Activation of this plugin on production instances may require a separate Performance Analytics license. Contact ServiceNow for details. | Active  | false          | • com.snc.pa  
• com.glide.awa |
| Performance Analytics - Content Pack - Application Portfolio Management | com.snc.pa.apm    | Application Portfolio Management dashboards developed using Performance analytics premium. | Inactive| true           | • com.snc.apm  
• com.snc.pa |
| Performance Analytics - Content Pack - Application Portfolio Management and Change Management | com.snc.pa.apm.change_request | Provides integration of Application Portfolio Management with Change Management which enables performance analytics dashboards of business applications associated with Change requests. Activation of this plugin on production instances may have licensing implications. Contact your ServiceNow account team for details. | Inactive| true           | • com.snc.apm  
• com.snc.pa  
• com.snc.pa.change |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
</table>
| Performance Analytics - Content Pack - Application Portfolio Management and Problem Management | com.snc.pa.apm.problem         | Provides integration of Application Portfolio Management with Problem Management which enables performance analytics dashboards of business applications. Activation of this plugin on production instances may have licensing implications. Contact your ServiceNow account team for details.                                                                 | Inactive | true           | • com.snc.apm  
  • com.snc.pa  
  • com.snc.pa.problem |
| Performance Analytics - Content Pack - Change Management             | com.snc.pa.change              | Provides Performance Analytics indicators and visualizations for Change Management. Activation of this plugin on production instances may require a separate Performance Analytics license. Contact ServiceNow for details.                                                                 | Inactive | false          | • com.snc.pa  
  • com.glideapp.report.itsm.change.overview |
| Performance Analytics - Content Pack - Cloud Management              | com.snc.pa.cmp                 | Provides Performance Analytics indicators and visualizations for Cloud Management. Activation of this plugin on production instances may require a separate Performance Analytics license. Contact ServiceNow for details.                                                                 | Inactive | false          | • com.snc.pa  
  • com.snc.runbook_automation.virtualization |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance Analytics - Content Pack - Cloud Resources (New in Quebec)</td>
<td>com.sn_disco_cd</td>
<td>Provides Performance Analytics indicators and visualizations for Cloud Resources. Activation of this plugin on production instances may require a separate Performance Analytics license. Contact ServiceNow for details.</td>
<td></td>
<td></td>
<td>• com.snc.pa&lt;br&gt;• com.sn_communities</td>
</tr>
<tr>
<td>Performance Analytics - Content Pack - Communities</td>
<td>com.snc.pa.communities</td>
<td>Provides Performance Analytics indicators and visualizations for Communities. Activation of this plugin on production instances may require a separate Performance Analytics license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.snc.pa&lt;br&gt;• com.snc.cmdb&lt;br&gt;• com.snc.pa.change</td>
</tr>
<tr>
<td>Performance Analytics - Content Pack - Configuration Management (CMDB)</td>
<td>com.snc.pa.cmdb</td>
<td>Provides Performance Analytics indicators and visualizations for Configuration Management (CMDB). Activation of this plugin on production instances may require a separate Performance Analytics license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.snc.pa&lt;br&gt;• com.snc.cmdb&lt;br&gt;• com.snc.pa.change</td>
</tr>
<tr>
<td>Performance Analytics - Content Pack - Content Analytics</td>
<td>com.snc.pa.premium.content</td>
<td>Analytics - Performance Analytics                                                                                                                                                                         Active</td>
<td>false</td>
<td>• com.sn_content_analytics&lt;br&gt;• com.snc.pa.premium</td>
<td></td>
</tr>
<tr>
<td>Performance Analytics - Content Pack - Content Automation</td>
<td>com.snc.pa.premium.content</td>
<td>Analytics - Content Automation Analytics                                                                                                                                                                    Active</td>
<td>false</td>
<td>• com.sn_content_analytics&lt;br&gt;• com.sn_content_automation&lt;br&gt;• com.snc.pa.premium</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-----------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glideapp.report.customer_service</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.sn_customerservice</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.pa.spotlight</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>Performance Analytics - Content Pack - Customer Service</td>
<td>com.snc.pa.customer_service</td>
<td>Provides Performance Analytics indicators and visualizations for Customer Service. Activation of this plugin on production instances may require a separate Performance Analytics license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.snc.pa&lt;br&gt;• com.glideapp.report.customer_service&lt;br&gt;• com.sn_customerservice&lt;br&gt;• com.sn_customerservice_pa</td>
</tr>
<tr>
<td>Performance Analytics - Content Pack - Discovery</td>
<td>com.snc.pa.discovery</td>
<td>Performance Analytics content pack for Discovery. Activation of this plugin on production instances may require a separate Performance Analytics license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.snc.pa&lt;br&gt;• com.snc.pa.cmdb&lt;br&gt;• com.snc.discovery</td>
</tr>
<tr>
<td>Performance Analytics - Content Pack - Event Management</td>
<td>com.snc.pa.em</td>
<td>Performance Analytics content pack for Event Management core. Activation of this plugin on production instances may require a separate Performance Analytics license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.snc.pa&lt;br&gt;• com.glideapp.itom.snac&lt;br&gt;• com.glideapp.report.em</td>
</tr>
<tr>
<td>Performance Analytics - Content Pack - Field Service Management</td>
<td>com.snc.work_management_pa</td>
<td>Provides Performance Analytics content for Field Service Management. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>true</td>
<td>• com.snc.pa&lt;br&gt;• com.snc.work_management</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance Analytics - Content Pack - Financial Management</td>
<td>com.snc.pa.fm</td>
<td>Provides Performance Analytics indicators and visualizations for Financial Management. Activation of this plugin on production instances may require a separate Performance Analytics license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.snc.financial_management • com.snc.pa</td>
</tr>
<tr>
<td>Performance Analytics - Content Pack - Financial Management for Field Service Management</td>
<td>com.snc.pa.fm.fsm</td>
<td>Enables Performance Analytics dashboards for Financial Management associated with Field Service Management. Activation of this plugin on production instances may require a separate Performance Analytics license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.snc.financial_management_for_fsm • com.snc.pa</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>----------------------------------------------------</td>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Performance Analytics - Content Pack - Financial Management for Financial Planning</td>
<td>com.snc.pa.financial_planning</td>
<td>Enables Performance analytics dashboards to associated to Financial Planning Process. Activation of this plugin on production instances may have licensing implications. Contact your ServiceNow account team for details.</td>
<td>Inactive</td>
<td>true</td>
<td>• com.snc.financial_planning • com.snc.pa</td>
</tr>
<tr>
<td>Performance Analytics - Content Pack - GRC: Audit Management</td>
<td>com.sn_audit_pa</td>
<td>Provides Performance Analytics reports for the GRC Audit Management application. Activation of this plugin on production will require a PA Premium license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.sn_grc_pa • com.sn_audit</td>
</tr>
<tr>
<td>Performance Analytics - Content Pack - GRC: Policy and Compliance Management</td>
<td>com.sn_compliance_pa</td>
<td>Provides Performance Analytics reports for the GRC Policy and Compliance Management application. Activation of this plugin on production will require a PA Premium license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.sn_grc_pa • com.sn_compliance</td>
</tr>
<tr>
<td>Performance Analytics - Content Pack - GRC: Risk Management</td>
<td>com.sn_risk_pa</td>
<td>Provides Performance Analytics reports for the GRC Risk Management application. Activation of this plugin on production will require a PA Premium license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.sn_grc_pa • com.sn_risk</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------------------------</td>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Performance Analytics - Content Pack -Vulnerability Response (Available in the ServiceNow Store)</td>
<td>sn_vul_analytics</td>
<td>Provides an integration of Vulnerability Response with Performance Analytics for trend-based reporting. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>true</td>
<td></td>
<td>• com.snc.pa • com.snc.treemap • sn_vul</td>
</tr>
<tr>
<td>Performance Analytics - Content Pack - Human Resources Lifecycle Events Scoped App</td>
<td>com.sn_hr_lifecycle_pa</td>
<td>Enables you to define and track key performance indicators (KPIs) for Enterprise Onboarding and Transitions and show these in scorecards and dashboards. Activation of this plugin on production will require a PA Premium license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>com.sn_hr_lifecycle_events</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------</td>
<td>---------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Performance Analytics - Content Pack - Human Resources Scoped App</td>
<td>com.sn_hr_pa</td>
<td>Enables you to define and track key performance indicators (KPIs) for HR and show these in scorecards and dashboards. Activation of this plugin on production will require a PA Premium license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>true</td>
<td>com.sn_hr_core</td>
</tr>
<tr>
<td>Performance Analytics - Content Pack - Incident SLA Management</td>
<td>com.snc.pa.sla</td>
<td>Performance Analytics content pack for Incident SLA Management. Activation of this plugin on production instances may require a separate Performance Analytics license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.pa</td>
</tr>
<tr>
<td>Performance Analytics - Content Pack - ITSM Dashboards</td>
<td>com.snc.pa.itsm_dashboards</td>
<td>Performance Analytics content pack for ITSM Dashboards. Activation of this plugin on production instances may require a separate Performance Analytics license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.snc.pa.change</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.pa.problem</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.pa.request</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.pa.request2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.pa.knowledge</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.pa.sla</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.pa.spotlight.incident</td>
</tr>
<tr>
<td>Performance Analytics - Content Pack - Knowledge Management</td>
<td>com.snc.pa.knowledge_v2</td>
<td>Performance Analytics content pack for Knowledge Management. Activation of this plugin on production instances may require a separate Performance Analytics license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.snc.pa</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.knowledge3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glideapp.report.knowledge.overview</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Performance Analytics - Content Pack - Operational Intelligence | com.snc.sa.metric.pa.content | Performance Analytics content pack for Analytics and Reporting Operational Intelligence Solution Dashboard and KPIs. Activation of this plugin on production instances may require a separate Performance Analytics license. Contact ServiceNow for details. | Inactive | false          | • com.snc.sa.metric  
• com.snc.pa  
• com.glideapp.canvas  
• com.snc.pa.em |
| Performance Analytics - Content Pack - Problem Management | com.snc.pa.problem          | Provides Performance Analytics indicators and visualizations for Problem Management. Activation of this plugin on production instances may require a separate Performance Analytics license. Contact ServiceNow for details. | Inactive | false          | • com.snc.pa  
• com.glideapp.report.itsm.problem.overview |
| Performance Analytics - Content Pack - PPM Standard Dashboards | com.snc.pa.pmo_dashboards   | Performance Analytics content pack for PPM Standard core. Activation of this plugin on production instances may require a separate Performance Analytics license. Contact ServiceNow for details. | Active  | false          | • com.snc.pps_dashboards  
• com.snc.financial_planning_pmo |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance Analytics - Content Pack - PPM Standard</td>
<td>com.snc.pps_dashboards</td>
<td>Performance Analytics content pack for Project Portfolio Suite Dashboards core. Activation of this plugin on production instances may require a separate Performance Analytics license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.snc.pa • com.snc.project_portfolio_suite</td>
</tr>
<tr>
<td>Performance Analytics - Content Pack - Request Management (Requested Item)</td>
<td>com.snc.pa.request</td>
<td>Performance Analytics content pack for Request Management for Requested Items. Installed with Performance Analytics - Premium. Activation of this plugin on production instances may require a separate Performance Analytics license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.pa</td>
</tr>
<tr>
<td>Performance Analytics - Content Pack - Request Management (Requests)</td>
<td>com.snc.pa.request2</td>
<td>Performance Analytics content pack for Request Management for Requests. Activation of this plugin on production instances may require a separate Performance Analytics license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.pa</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------------------------------</td>
<td>---------</td>
<td>---------------</td>
<td>--------------------------------------------------</td>
</tr>
</tbody>
</table>
| Performance Analytics - Content Pack - Service Desk Chat | com.snc.pa.chat           | Provides Performance Analytics indicators and visualizations for Service Desk Chat. Activation of this plugin on production instances may require a separate Performance Analytics license. Contact ServiceNow for details. | Inactive| false          | • com.glide.connect  
• com.glide.connect.support  
• com.glide.connect.managers_dashboard  
• com.snc.pa |
| Performance Analytics - Content Pack - Service Mapping | com.snc.service-mapping.pa.content | Performance Analytics content pack for Service Mapping Dashboard and KPIs. Activation of this plugin on production instances may require a separate Performance Analytics license. Contact ServiceNow for details. | Inactive| false          | • com.snc.pa  
• com.snc.pa.cmdb |
| Performance Analytics - Content Packs for ITSM        | com.snc.premium.all_content | Installing this plugin installs content packs for Incident, Problem, Change, Incident SLA, Knowledge, and Requested Items for Performance Analytics. | Inactive| false          | • com.snc.pa.change  
• com.snc.pa.problem  
• com.snc.pa.request  
• com.snc.pa.request2  
• com.snc.pa.knowledge  
• com.snc.pa.sla |
<p>| Performance Analytics - Content Pack - Time Card Management | com.snc.pa.time_card      | Performance Analytics content pack for Time card management. Activation of this plugin on production instances may require a separate Performance Analytics license. Contact ServiceNow for details. | Active  | false          | com.snc.pa |</p>
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
</table>
| Performance Analytics - Context Sensitive Analytics for Change Management | com.snc.pa.change.context_sensitive_analytics | Provides additional ability to open Performance Analytics context sensitive Performance Analytics dashboards in change request form based on UI actions. | Inactive | false | • com.snc.pa  
• com.snc.pa.change |
| Performance Analytics - Context Sensitive Analytics for Chat | com.snc.pa.chat.context_sensitive_analytics | Provides additional dashboard to analyze Connect Support metrics for support queues in Performance Analytics. Adds a related link to the Chat Queue Entry [chat_queue_entry] form to quickly display Performance Analytics metrics for the associated queue. | Inactive | false | • com.snc.pa  
• com.snc.pa.chat |
| Performance Analytics - Context Sensitive Analytics for Customer Service | com.snc.pa.cs.context_sensitive_analytics | Performance Analytics adding ability to open Performance Analytics context-sensitive dashboards in customer service form based on UI actions. | Inactive | false | • com.snc.pa  
• com.snc.pa.customer_service  
• com.sn.customerservice  
• com.snc.pa.customer_service |
<p>| Performance Analytics - Context Sensitive Analytics for Incident | com.snc.pa.incident.context_sensitive_analytics | Performance Analytics adding ability to open Performance Analytics context-sensitive dashboards in incident form based on UI actions. | Inactive | false | com.snc.pa |</p>
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
</table>
| Performance Analytics - Context Sensitive Analytics for Problem Management | com.snc.pa.problem.context_sensitive_analytics | Performance Analytics adding ability to open Performance Analytics context sensitive Performance Analytics dashboards in problem form based on UI actions. | Inactive | false | • com.snc.pa  
• com.snc.pa.problem |
| Performance Analytics - Data Collector. (Deprecated.) Use plugin Performance Analytics instead | com.snc.pa.dc          | Data Collector for Performance Analytics. Deprecated. Use plugin Performance Analytics instead. | Inactive | false | |
| Performance Analytics - Diagnostics              | com.snc.pa.diagnostics | Enables users to run diagnostics on Performance Analytics records and related applications. | Active | false | com.snc.pa |
| Performance Analytics - Domain Support           | com.snc.pa.domain_support | The Performance Analytics Domain Support plugin provides additional features to support scores collection on domain separated instances. This plugin requires the Domain Separation plugin to be installed. | Active | false | • com.snc.pa.premium  
• com.glideapp.dashboards  
• com.glide.domain.msp_extensions.installer |
<p>| Performance Analytics - Example - LinkedIn      | com.snc.pa.linkedin    | Automatically imports LinkedIn data historically and daily.                 | Inactive | false | com.snc.pa |
| Performance Analytics - Example - Stocks Quotes   | com.snc.pa.stock       | Automatically imports stock quotes data historically and daily.             | Inactive | false | com.snc.pa |</p>
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance Analytics - Example - Twitter</td>
<td>com.snc.pa.twitter</td>
<td>Automatically import Twitter data historically and daily.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.pa</td>
</tr>
<tr>
<td>Performance Analytics - PA Solution Library</td>
<td>com.snc.pa.solution.library</td>
<td>Allows you to upgrade the visuals of dashboards that are shipped in other content packs. Upgrade or duplicate whole dashboards or selected elements.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.pa</td>
</tr>
</tbody>
</table>
| Performance Analytics - Premium                  | com.snc.pa.premium  | Enables the functionality provided by the fully licensed version of Performance Analytics. Requires additional fee. Functionality includes the ability to:  
• Create indicators, breakdowns, and other records  
• Create interactive filters and use interactive analysis  
• Create text analytics widgets  
• Use Performance Analytics with external data  
• Preserve scores beyond 180 days | Inactive | false          | com.snc.pa   |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance Analytics - Scores Migration</td>
<td>com.snc.pa.scores_migration</td>
<td>Installing this plugin will migrate scores from old tables to new tables. To provide optimal performance, the Scores [pa_scores] table is being migrated to Scores Level 1 [pa_scores_11] and Scores Level 2 [pa_scores_12]. During migration you cannot collect, modify, or delete scores. Scheduled data collection and cleanup jobs will not run during migration.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.pa</td>
</tr>
<tr>
<td>Performance Analytics - Spotlight</td>
<td>com.snc.pa.spotlight</td>
<td>Enables records to be ranked by multiple weighted criteria. When a record surpasses a threshold of total weights, a Spotlight is created to highlight that record.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.pa</td>
</tr>
</tbody>
</table>
| Performance Analytics - Spotlight - change spotlight content pack | com.snc.pa.spotlight.change | Provides preconfigured Spotlight components and a dashboard to identify and prioritize Change records according to multiple weighted criteria. Requires fully licensed Performance Analytics. | Inactive | false          | com.snc.pa.spotlight  
<p>|                                 |                             |                                                                             |         |                | com.snc.pa.change     |</p>
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance Analytics - Spotlight - Incident Spotlight content pack</td>
<td>com.snc.pa.spotlight.incident</td>
<td>Provides preconfigured Spotlight components and a dashboard to identify and prioritize Incident records according to multiple weighted criteria.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.snc.pa.spotlight</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glideapp.canvas</td>
</tr>
<tr>
<td>Performance Analytics - Spotlight - Problem spotlight content pack</td>
<td>com.snc.pa.spotlight.problem</td>
<td>Provides preconfigured Spotlight components and a dashboard to identify and prioritize Problem records according to multiple weighted criteria. Requires fully licensed Performance Analytics.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.snc.pa.spotlight</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.pa.problem</td>
</tr>
<tr>
<td>Performance Analytics - Spotlight - Request spotlight content pack</td>
<td>com.snc.pa.spotlight.request</td>
<td>Provides preconfigured Spotlight components and a dashboard to identify and prioritize Request records according to multiple weighted criteria. Requires fully licensed Performance Analytics.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.snc.pa.spotlight</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.pa.request2</td>
</tr>
<tr>
<td>Performance Analytics and Reporting - Service Portal Widgets</td>
<td>com.snc.pa.sp.widget</td>
<td>Support for Performance Analytics widgets in the Service Portal. A number of JavaScript and CSS libraries are included to be able to run Performance Analytics widgets independently in the Service Portal.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.service-portal</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Performance Analytics Content Pack for Major Incident Management</td>
<td>com.snc.pa.incident.mim</td>
<td>Provides Performance Analytics indicators and visualizations for identifying and tracking major incidents. Extended functionality available with fully licensed Performance Analytics.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.incident.mim</td>
</tr>
<tr>
<td>Performance Analytics Usage Overview</td>
<td>com.snc.pa.usage.overview</td>
<td>This plugin contains dashboards, reports, and indicators to monitor Performance Analytics and Reporting usage.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.pa</td>
</tr>
</tbody>
</table>
| Performance Analytics Premium                   | com.snc.pa.premium          | Enables the functionality that you are entitled to with a subscription to Performance Analytics across all ServiceNow® products. Requires additional fee. Functionality includes the ability to:  
  • Create indicators, breakdowns, and other records  
  • Create interactive filters and use interactive analysis  
  • Create text analytics widgets  
  • Use Performance Analytics with external data  
  • Preserve scores beyond 180 days | Inactive | false          | com.snc.pa               |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance Analytics and Reporting - Service Portal Widgets</td>
<td>com.snc.pa.sp.widget</td>
<td>Support for Performance Analytics widgets in the Service Portal. A number of JavaScript and CSS libraries are included to be able to run Performance Analytics widgets independently in the Service Portal.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.service-portal</td>
</tr>
</tbody>
</table>
| Performance Analytics Premium for APM     | com.snc.pa.premium.apm | Enables the Performance Analytics functionality that you are entitled to with a subscription that includes APM and Performance Analytics. Requires additional fee. Functionality includes the ability to:  
• Create indicators, breakdowns, and other records  
• Create interactive filters and use interactive analysis  
• Create text analytics widgets  
• Use Performance Analytics with external data  
• Preserve scores beyond 180 days                  | Inactive | false          | com.snc.pa                    |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
</table>
| Performance Analytics Premium for Business Management | com.snc.pa.premium.itbm | Enables the Performance Analytics functionality that you are entitled to with a subscription that includes Business Management and Performance Analytics. Requires additional fee. Functionality includes the ability to:  
• Create indicators, breakdowns, and other records  
• Create interactive filters and use interactive analysis  
• Create text analytics widgets  
• Use Performance Analytics with external data  
• Preserve scores beyond 180 days | Inactive | false | com.snc.pa |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
</table>
| Performance Analytics                       | com.snc.pa.premium  | Enables the Performance Analytics functionality that you are entitled to with a subscription that includes Cloud Control Center and Performance Analytics. Requires additional fee. Functionality includes the ability to:  
• Create indicators, breakdowns, and other records  
• Create interactive filters and use interactive analysis  
• Create text analytics widgets  
• Use Performance Analytics with external data  
• Preserve scores beyond 180 days       | Inactive           | false                        | com.snc.pa      |              |              |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
</table>
| Performance Analytics Premium for Customer Service | com.snc.pa.premium.cs | Enables the Performance Analytics functionality that you are entitled to with a subscription that includes Customer Service and Performance Analytics. Requires additional fee. Functionality includes the ability to:  
  • Create indicators, breakdowns, and other records  
  • Create interactive filters and use interactive analysis  
  • Create text analytics widgets  
  • Use Performance Analytics with external data  
  • Preserve scores beyond 180 days | Inactive   | false               | com.snc.pa       |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
</table>
| Performance Analytics Premium for Financial Management | com.snc.pa.premium.fm    | Enables the Performance Analytics functionality that you are entitled to with a subscription that includes Financial Management and Performance Analytics. Requires additional fee. Functionality includes the ability to:  
• Create indicators, breakdowns, and other records  
• Create interactive filters and use interactive analysis  
• Create text analytics widgets  
• Use Performance Analytics with external data  
• Preserve scores beyond 180 days                                                                                                   | Inactive | false          | com.snc.pa     |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
</table>
| Performance Analytics Premium for Human Resource Management | com.snc.pa.premium.hr | Enables the Performance Analytics functionality that you are entitled to with a subscription that includes Human Resource Management and Performance Analytics. Requires additional fee. Functionality includes the ability to:  
• Create indicators, breakdowns, and other records  
• Create interactive filters and use interactive analysis  
• Create text analytics widgets  
• Use Performance Analytics with external data  
• Preserve scores beyond 180 days | Inactive | false           | com.snc.pa      |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
</table>
| Performance Analytics Premium for IT Operations Management | com.snc.pa.premium.itom | Enables the Performance Analytics functionality that you are entitled to with a subscription that includes ITOM and Performance Analytics. Requires additional fee. Functionality includes the ability to:  
• Create indicators, breakdowns, and other records  
• Create interactive filters and use interactive analysis  
• Create text analytics widgets  
• Use Performance Analytics with external data  
• Preserve scores beyond 180 days | Inactive     | false           | com.snc.pa     |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance Analytics Premium for IT Operations Suite</td>
<td>com.snc.pa.premium.itos</td>
<td>Enables the Performance Analytics functionality that you are entitled to with a subscription that includes IT Operations Suite and Performance Analytics. Requires additional fee. Functionality includes the ability to: • Create indicators, breakdowns, and other records • Create interactive filters and use interactive analysis • Create text analytics widgets • Use Performance Analytics with external data • Preserve scores beyond 180 days</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.pa</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>---------------</td>
</tr>
</tbody>
</table>
| Performance Analytics Premium for Project Portfolio Management | com.snc.pa.premium.ppm | Enables the Performance Analytics functionality that you are entitled to with a subscription that includes PPM and Performance Analytics. Requires additional fee. Functionality includes the ability to:  
  • Create indicators, breakdowns, and other records  
  • Create interactive filters and use interactive analysis  
  • Create text analytics widgets  
  • Use Performance Analytics with external data  
  • Preserve scores beyond 180 days | Inactive | false          | com.snc.pa     |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
</table>
| Performance Analytics Premium for Security Incident Response | com.snc.pa.premium.sir | Enables the Performance Analytics functionality that you are entitled to with a subscription that includes SIR and Performance Analytics. Requires additional fee. Functionality includes the ability to:  
• Create indicators, breakdowns, and other records  
• Create interactive filters and use interactive analysis  
• Create text analytics widgets  
• Use Performance Analytics with external data  
• Preserve scores beyond 180 days | Inactive | false | com.snc.pa |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance Analytics Premium for Security Operations</td>
<td>com.snc.pa.premium.sir</td>
<td>Enables the Performance Analytics functionality that you are entitled to with a subscription that includes Security Operations and Performance Analytics. Requires additional fee. Functionality includes the ability to: • Create indicators, breakdowns, and other records • Create interactive filters and use interactive analysis • Create text analytics widgets • Use Performance Analytics with external data • Preserve scores beyond 180 days</td>
<td>Active</td>
<td>false</td>
<td>com.snc.pa</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Performance Analytics Premium for Service Management</td>
<td>com.snc.pa.premium.service</td>
<td>Performance Analytics functionality that you are entitled to with a subscription that includes Service Management and Performance Analytics. Requires additional fee. Functionality includes the ability to: • Create indicators, breakdowns, and other records • Create interactive filters and use interactive analysis • Create text analytics widgets • Use Performance Analytics with external data • Preserve scores beyond 180 days</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.pa</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------</td>
<td>----</td>
<td>-------------</td>
<td>--------</td>
<td>----------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Performance Analytics Premium for Service Watch Insight</td>
<td>com.snc.pa.premium.swi</td>
<td>Enables the Performance Analytics functionality that you are entitled to with a subscription that includes Service Watch Insight and Performance Analytics. Requires additional fee. Functionality includes the ability to:  • Create indicators, breakdowns, and other records  • Create interactive filters and use interactive analysis  • Create text analytics widgets  • Use Performance Analytics with external data  • Preserve scores beyond 180 days</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.pa</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>----------------------------</td>
</tr>
</tbody>
</table>
| Performance Analytics Premium for Software Asset Management | com.snc.pa.premium.sam      | Enables the Performance Analytics functionality that you are entitled to with a subscription that includes Software Asset Management and Performance Analytics. Requires additional fee. Functionality includes the ability to:  
• Create indicators, breakdowns, and other records  
• Create interactive filters and use interactive analysis  
• Create text analytics widgets  
• Use Performance Analytics with external data  
• Preserve scores beyond 180 days | Inactive | false            | com.snc.pa     |
| Performance Dashboards                      | com.glide.performance_dashboards | Performance Dashboards                                                                                                                                                                                      | Active  | false          | com.glide.cms         |
| Performance Metrics for VTB                 | com.glide.ui.vtb_metrics    | Provides profiler page for benchmarking Java methods in Visual Task Board.                                                                                                                                    | Inactive | false          | com.glide.ui.vtb     |
| Platform as a Service                       | com.snc.paas                | Allows the development of custom applications to meet business needs.                                                                                                                                        | Active  | false          | com.glideapp.workflow |

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Playbooks for Customer Service Management</td>
<td>com.sn_csm_playbook</td>
<td>Playbooks for Customer Service Management guides customer service agents through the various tasks and their sequence to resolve customer issues and visualizes the entire lifecycle across diverse and siloed processes.</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.pad.core • com.glide.playbook_experience.config • com.sn_customerservice</td>
</tr>
<tr>
<td>Portfolio Management</td>
<td>com.snc.portfolio_management</td>
<td>The Portfolio Management plugin.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>PPM Mobile</td>
<td>com.sn_ppm.mobile</td>
<td>This plugin provides Project Portfolio Suite Mobile user experience. This provides access to project status and project status report in the agent mobile application. PPM Standard is required. But if it is not active, installing PPM Mobile also activates PPM Standard plugin.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.financial_planning_pmo</td>
</tr>
<tr>
<td>PPM Ridac</td>
<td>com.snc.ppm_ridac</td>
<td>The PPM RIDAC flow actions plugin. Installs the flow actions needed for RIDAC conversions.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>PPM Standard Multicurrency</td>
<td>com.snc.ppm_multicurrency</td>
<td>Enable advanced ability to manage PPM financials in multiple currencies.</td>
<td>Inactive</td>
<td>true</td>
<td>• com.snc.financial_planning_pmo • com.glide.currency2</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Predictive Intelligence</td>
<td>com.glide.platform_ml</td>
<td>This is the new name for the Agent Intelligence plugin, effective in the New York release and beyond. Predictive Intelligence enables the creation of machine learning solutions using data in your instance. The plugin provides various capabilities and solution types for training the system to predict, recommend, and drive data outcomes.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.platform_ml_pa</td>
</tr>
<tr>
<td>Predictive Intelligence - Enhanced UI</td>
<td>com.snc.ml_ui</td>
<td>This plugin enhances the UI for Predictive Intelligence.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
</tbody>
</table>
| Predictive Intelligence for Contextual Search | com.snc.contextual_search_ml   | Enables customers to leverage machine-learning algorithms for searching with Contextual Search. For example: Similar Open Incidents. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.                                      | Inactive| false          | • com.snc.contextual_search  
• com.glide.platform_ml                                                      |
| Predictive Intelligence for Customer Service Management | com.snc.csm_ml   | Enables customers to leverage machine learning algorithms for searching related cases in Customer Service Management. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.                                      | Inactive| false          | • com.sn_customerservice  
• com.snc.contextual_search_ml  
• com.snc.adv_exs_results_email_script                                       |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Predictive Intelligence for Field Service Management</td>
<td>com.snc.fsm_ml</td>
<td>Provides various capabilities driven by machine-learning solutions. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Active</td>
<td>true</td>
<td>• com.snc.work_management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.contextual_search_ml</td>
</tr>
<tr>
<td>Predictive Intelligence for Incident</td>
<td>com.snc.incident.ml</td>
<td>Enables customers to leverage machine-learning algorithms with application logic for predicting Open change request and Open Problem for Incident. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.contextual_search_ml</td>
</tr>
<tr>
<td>Predictive Intelligence for Incident Management</td>
<td>com.snc.incident.ml_solution</td>
<td>Predictive Intelligence for Incident Management provides solution definitions as templates so that you can build models without writing any code.</td>
<td>Inactive</td>
<td>false</td>
<td>NA</td>
</tr>
<tr>
<td>Predictive Intelligence for Major Incident Management</td>
<td>com.snc.incident.mim.ml_solution</td>
<td>Predictive Intelligence for Major Incident Management provides solution definitions as templates so that you can build models without writing any code.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.snc.incident.mim</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.incident.ml_solution</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Predictive Intelligence for Knowledge Management</td>
<td>com.snc.knowledge_ml</td>
<td>Provides various capabilities driven by machine-learning solutions. For example, capabilities such as similar articles and knowledge demand insights. Activation of this plugin on production instances may require a separate license. Contact for details.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.contextual_search_ml</td>
</tr>
<tr>
<td>Predictive Intelligence for PPM (Available in the ServiceNow Store)</td>
<td>com.snc.ppm_ml</td>
<td>The Predictive Intelligence for Project Management capability uses machine-learning algorithms to search and display similar projects and demands.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.contextual_search_ml, com.snc.financial_planning_pmo</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Predictive Intelligence for Universal Request (New in Quebec)</td>
<td>com.snc.universal_request.ml</td>
<td>Contains the machine learning solutions for the Universal Request use cases.</td>
<td>Active</td>
<td>false</td>
<td>• com.snc.universal_request</td>
</tr>
<tr>
<td>Predictive Intelligence Incident Estimated Time to Resolve (New in Quebec)</td>
<td>com.snc.incident.ml.ettr</td>
<td>Enables customers to leverage machine-learning algorithms with application logic for predicting the estimated time to resolve for an Incident. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.glide.platform_ml • com.sn_itsm_ettr_card</td>
</tr>
<tr>
<td>Predictive Intelligence Workbench HRSD Content</td>
<td>com.sn_piwb_hrsd_content</td>
<td>Enables customers to seed HRSD specific content to provide implementation guidance for use cases created through Predictive Intelligence Workbench.</td>
<td>Active</td>
<td>false</td>
<td>• com.sn_hr_core • com.glide.platform_ml</td>
</tr>
<tr>
<td>Predictive Intelligence Reports</td>
<td>com.glide.platform_ml_pa</td>
<td>This is the new name for the Agent Intelligence Reports plugin.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Predictive Intelligence Workbench</td>
<td>com.sn_piwb_ml</td>
<td>Predictive Intelligence Workbench core plugin provides a common framework for creating use case templates, managing use cases and dashboard to communicate value across all SN apps</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.platform_ml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.platform_ml_pa</td>
</tr>
<tr>
<td>Proactive Customer Service Operations</td>
<td>com.snc.proactive_cs_ops</td>
<td>Enables customers to create cases proactively from alerts either manually or through automation and track the accounts and the corresponding install base items affected by the alert.</td>
<td>Active</td>
<td>false</td>
<td>• com.sn_majorissue_mgt</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.install_base</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glideapp.itom.snac</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.sn_cs_sm_request</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.csm_action_status</td>
</tr>
<tr>
<td>Proactive Customer Service Operations with Event Management</td>
<td>com.snc.proactive_cs_itom</td>
<td>Provides an integration between Customer Service Management and ITOM Event Management. Enables customers to create cases proactively from alerts either manually or through automation and track the accounts and the corresponding install base items affected by the alert.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.snc.proactive_cs_ops</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glideapp.itom.snac</td>
</tr>
<tr>
<td>Problem Management</td>
<td>com.snc.problem</td>
<td>Helps to identify the cause of a service interruption reported by a significant or recurring incidents.</td>
<td>Active</td>
<td>true</td>
<td>• com.snc.service</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glideapp.report.itsm.problem.overview</td>
</tr>
<tr>
<td>Problem Management — ATF Tests</td>
<td>com.snc.problem.atf</td>
<td>Delivers ATF tests for Problem Management.</td>
<td>Active</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>Problem Overview Homepage</td>
<td>com.glideapp.report.itsm.problem.overview</td>
<td>Displays Problem overview homepage.</td>
<td>Active</td>
<td>false</td>
<td>com.glideapp.report</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Problem Management Best Practice - Madrid                             | com.snc.best_practice.problem.madrid | Helps to identify the cause of a service interruption reported by a significant or recurring incidents. Provides roles for problem management including a problem coordinator, problem manager and problem administrator. Provides fields to record the category, where the issue was first reported, the workaround, the cause notes and the fix notes. Searches for and attaches knowledge articles. Communicates when a workaround or fix is available. | Active   | true           | • com.snc.problem  
• com.snc.problem_task                                                                                                                     |
| Problem Management Best Practice - Madrid - Knowledge Integration     | com.snc.best_practice.problem.madrid.knowledge | Helps to identify the cause of a service interruption reported by a significant or recurring incidents. Create Known Error articles for Incident Deflection (requires Knowledge Management Advanced plugin to be activated).                                                                                                                                                                                                                          | Active   | true           | • Problem Management Best Practice - Madrid (com.snc.best_practice.problem.madrid)  
• Knowledge Management Advanced Installer (com.snc.knowledge_advanced.installer)                              |
| Problem Management Best Practice - Madrid - State Model               | com.snc.best_practice.problem.madrid.state_model | Provides support for state management to control how a problem or problem task is allowed to transition through a predefined list of states.                                                                                                                                                                                                                                                                                           | Inactive | true           | Problem Management Best Practice - Madrid (com.snc.best_practice.problem.madrid) |

© 2021 ServiceNow, Inc. All rights reserved. ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problem Tasks</td>
<td>com.snc.problem_task</td>
<td>Adds a Problem Task table with a reference to the Problem table.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Process Automation Designer for ITSM</td>
<td>com.snc.itsm.playbook</td>
<td>Process Automation Designer enables business process owners to consolidate multiple flows across the enterprise into a single unified process. Process owners can create and manage cross-functional automated processes to provide end-users with a simplified, task-oriented interface to guide them through these processes, such as playbooks in Agent Workspace. Process Automation Designer for ITSM enables process owners to create and manage the cross-functional IT process flows.</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.pad.core</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.playbook_experience</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.incident</td>
</tr>
<tr>
<td>Process Flow Formatter</td>
<td>com.snc.process_flow_formatter</td>
<td>Quickly summarizes multiple pieces of information about a process and displays the stages graphically at the top of a form.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Process Optimization</td>
<td>com.sn_process_optimization</td>
<td>Creates business process flows from the data in audit trails. This allows in-depth analysis of business processes to improve outcomes.</td>
<td>Active</td>
<td>false</td>
<td>• com.agent_workspace</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.workspace_core</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.devsnc_sn_promin_workbench</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Process Optimization Content Pack for CSM   | com.snc.csm_process_optimization | Provides pre-configured process optimization models and improvement initiatives for the CSM Processes.                                                                                                     | Inactive| false          | • com.sn_customerservice  
• com.sn_process_optimization                                                                        |
| Process Optimization Workspace              | com.sn_po_workspace          | Delivers the Process Optimization workspace feature for analyst users.                                                                                                                                       | Inactive| false          | • com.agent_workspace  
• com.sn_process_optimization  
• com.sn_po_workspace_components                                                                 |
| Procurement                                 | com.snc.procurement            | Allows users to create purchase orders and obtain items for fulfilling service catalog requests.                                                                                                              | Inactive| true           |                                                                                                        |
| Product Catalog                             | com.snc.product_catalog       | Provides information about individual models. Models are specific versions or various configurations of an asset. Models published to the product catalog are automatically published to the service catalog. | Active  | true           |                                                                                                        |
| Program Common                              | com.snc.program_common        | The Program Common plugin aids in planning, organizing and managing programs with basic features.                                                                                                            | Active  | false          | • com.snc.planned_task_v2  
• com.snc.itbm_security                                                                     |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
</table>
| Project Management      | com.snc.project_management_v3| **Description**: Project Management application aids in planning, organizing and managing projects and resources in order to setup, execute, and complete a project faster and easier. Only upgrade is allowed for this plugin. Activation should be done through PPM Standard plugin. | Inactive | true            | • com.snc.project_management_delete_v3
• com.glide.schedules
• com.snc.planned_task_v2
• com.snc.time_card
• com.snc.skills_management
• com.snc.process_flow_formatter
• com.snc.cost_management
• com.snc.project_management_db_views
• com.snc.project_workbench
• com.snc.timeline_visualization
• com.glide.ui.checklist |
<p>| Project Management      | com.snc.ppm_teamspace_1       | <strong>Description</strong>: Installs a Project TeamSpace so that each team or each department like Marketing, Finance, IT-Team1, IT-Team2 can implement PPM suitable to their needs without overstepping each other. | Inactive | true            | com.snc.financial_planning_pmo                                               |
| Project Management      | com.snc.ppm_teamspace_2       | <strong>Description</strong>: Installs a Project TeamSpace so that each team or each department like Marketing, Finance, IT-Team1, IT-Team2 can implement PPM suitable to their needs without overstepping each other. | Inactive | false           | com.snc.financial_planning_pmo                                               |
| Project Management      | com.snc.ppm_teamspace_3       | <strong>Description</strong>: Installs a Project TeamSpace so that each team or each department like Marketing, Finance, IT-Team1, IT-Team2 can implement PPM suitable to their needs without overstepping each other. | Inactive | false           | com.snc.financial_planning_pmo                                               |</p>
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Management TeamSpace 4</td>
<td>com.snc.ppm_teamspace_4</td>
<td>Installs a Project TeamSpace so that each team or each department like Marketing, Finance, IT-Team1, IT-Team2 can implement PPM suitable to their needs without overstepping each other.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.financial_planning_pmo</td>
</tr>
<tr>
<td>Project Management TeamSpace 5</td>
<td>com.snc.ppm_teamspace_5</td>
<td>Installs a Project TeamSpace so that each team or each department like Marketing, Finance, IT-Team1, IT-Team2 can implement PPM suitable to their needs without overstepping each other.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.financial_planning_pmo</td>
</tr>
<tr>
<td>Project Portfolio Suite</td>
<td>com.snc.project_portfolio_suite</td>
<td>The Project Portfolio Suite (PPS) plugin activates an integrated set of applications for project portfolio management and IT software development. Only upgrade is allowed for this plugin. Activation should be done through PPM Standard plugin.</td>
<td>Inactive</td>
<td>true</td>
<td>• com.snc.project_management_v3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.demand_management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.resource_management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.test_mgmt</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.sdli.scru.ppm_int</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.test_mgmt.ppm_int</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.program_management</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>---------------------------------------------------------</td>
</tr>
<tr>
<td>PPM Standard</td>
<td>com.snc.financial_planning_pmo</td>
<td>Enables you to manage your demands, resources, portfolios and projects, and gives full visibility from idea to execution. It also helps you plan, track, and manage cost and budget on projects and demands in a portfolio to strike a balance between investment and returns. Agile management and test management help you to improve productivity and service delivery.</td>
<td>Inactive</td>
<td>true</td>
<td>• com.snc.project_portfolio_suite • com.snc.financial_planning • com.snc.rate_model</td>
</tr>
<tr>
<td>PPM Standard - ATF Tests</td>
<td>com.snc.financial_planning_pmo.atf</td>
<td>ATF tests for PPM Standard</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Protocol Profile Manager</td>
<td>com.glide.protocol_profile</td>
<td>Defines properties associated to protocols such as default port and keystore.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Proxy Agent for connecting to Natural Language Understanding providers</td>
<td>com.glide.nlu.proxy</td>
<td>The base NLU proxy agent for connecting to NLU providers. Intended for use by Virtual Agent and other clients.</td>
<td>Active</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>Proxy Agent to the IBM Watson Natural Language Understanding server</td>
<td>com.glide.nlu.ibmwatson.intent.discovery</td>
<td>Activates the IBM Watson Assistant Intent and Entity integration, which enables Virtual Agent to use intents, entities, and utterances defined in IBM Watson Assistant.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.nlu.proxy</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>----------------------------------------------------</td>
<td>-----------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>Proxy Agent to the Microsoft LUIS Natural Language Understanding server</td>
<td>com.glide.nlu.msluis.intent.discovery</td>
<td>Proxy agent to the Microsoft LUIS Natural Language Understanding server.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.nlu.intent.discovery</td>
</tr>
<tr>
<td>Proxy Agent to the ServiceNow Natural Language Understanding server</td>
<td>com.glide.nlu.intent.discovery</td>
<td>Proxy agent for connecting to ServiceNow's NLU server for NLU intent discovery. Intended for use by Virtual Agent and other clients.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.nlu.proxy</td>
</tr>
<tr>
<td>Push Feedback</td>
<td>com.glide.push.feedback</td>
<td>Collects feedback from the Apple push notification service or another feedback service. Provides a REST API for other instances to collect from this service.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.push</td>
</tr>
<tr>
<td>Push Notification</td>
<td>com.glide.push</td>
<td>Defines push notification message enqueuing and sending Responsible for processing push notifications to their next destination.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Push Retention</td>
<td>com.glide.push_retention</td>
<td>Provides retention policy for push notifications.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.push</td>
</tr>
<tr>
<td>Qualys Vulnerability Integration (Available in the ServiceNow Store)</td>
<td>snc_vul_qualys</td>
<td>Provides the ability to integrate the ServiceNow Vulnerability Response application with the Qualys vulnerability scanner. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>snc_vul</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Query Rules (New in Quebec)</td>
<td>com.snc.query_rules</td>
<td>Plugin that brings in the table and the logic needed to generate encoded queries per table for a user based on the roles the user has.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Query stats</td>
<td>com.glide.stats.query</td>
<td>Query stats.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.stats</td>
</tr>
<tr>
<td>Quick Actions</td>
<td>com.glide.quickactions</td>
<td>Enables slash commands in Agent Workspace chat.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
</tbody>
</table>
| Quiz Designer                                   | com.glide.quiz_designer  | Provides the ability to send scored questionnaires quickly and easily to one or more users. A quiz may have categories of questions that are assigned only to some users.                                                                                                                                                                                   | Inactive | false          | • com.glide.assessment_designer.common  
• com.snc.assessment_core                                                                 |
<p>| Random Watermark Support                        | com.glide.email.random_watermark | Generate unpredictable watermarks, and enable matching on these watermarks in inbound emails.                                                                                                                                                                                                                                                    | Active | false          | com.glide.mailbox                                                                 |
| Rapid7 Vulnerability Integration (Available in the ServiceNow Store) | sn_vul_t7 | Provides the ability to integrate the ServiceNow Vulnerability Response application with the Rapid7 Nexpose and InsightVM products. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.                                                                                                                          |        |                | sn_vul                                                                 |
| Rate Limit for REST API                         | com.glide.rest.rate_limit| Rate Limit support for REST API                                                                                                                                                                                                                                                                                                                   | Active | true           |                                                                                   |</p>
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read only roles for Application Portfolio Management</td>
<td>com.snc.apm_read_roles</td>
<td>The plugin provides read only roles for Application Portfolio Management.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Read only roles for PPM Standard</td>
<td>com.snc.pmo_read_roles</td>
<td>Read only roles for PPM Standard.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Read-Only User Role</td>
<td>com.snc.read_only.role</td>
<td>Enables Read-Only user role functionality.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Relationship Layout</td>
<td>com.glide.ui.relationship_layout</td>
<td>Enables scoped relationships to be associated to out-of-scope related list views.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Release Management</td>
<td>com.snc.release_management</td>
<td>The Release Management v2 plugin is a rewrite of the original release management module. All products, releases, features, and release tasks are planned_task extensions, and much of the project management functionality (Gantt charts, timelines, time cards) is shared with release.</td>
<td>Active</td>
<td>true</td>
<td>com.snc.release_management com.snc.planned_task com.snc.process_flow_formatter</td>
</tr>
<tr>
<td>Remote Tables</td>
<td>com.glide.script.vtable_demo</td>
<td>Supports remote tables and associated script definitions that can be used to retrieve and optionally cache data from external sources.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report - PDF Page Header Footer Templates</td>
<td>com.glideapp.report_page_hdrftr</td>
<td>Allows the user to configure and store page headers and footers for PDF reports.</td>
<td>Active</td>
<td>false</td>
<td>com.glideapp.report com.glideapp.report2</td>
</tr>
<tr>
<td>Report Charting v2</td>
<td>com.glideapp.report.charting_v2</td>
<td>Installs V2 of ServiceNow charts with HighCharts.</td>
<td>Active</td>
<td>false</td>
<td>com.glideapp.report com.glideapp.report2</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Engine - use summary table for reports</td>
<td>com.glideapp.summary_report</td>
<td>Compresses the data from all reports, custom and standard, to be stored in the sys_report_summary table and separates the data from the rendering process for all reports. Report data is periodically purged from the sys_report_summary table (approximately every two hours).</td>
<td>Active</td>
<td>false</td>
<td>com.glideapp.report2</td>
</tr>
<tr>
<td>Report Security - enforce access control checks</td>
<td>com.glideapp.report_security</td>
<td>Enforces ACL checks when reports are created, deleted or updated.</td>
<td>Active</td>
<td>false</td>
<td>• com.glideapp.report&lt;br&gt;• com.glideapp.report2</td>
</tr>
<tr>
<td>Reporting Statistics Reports</td>
<td>com.glideapp.report_statreport</td>
<td>Provides reports and dashboards on reporting statistics.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glideapp.report</td>
</tr>
<tr>
<td>Required Form Fields</td>
<td>com.snc.required_form_fields</td>
<td>Allows an administrator to specify required fields that cannot be removed from a form.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Resource Management</td>
<td>com.snc.resource_management</td>
<td>Enables resource requesters and resource managers to plan, organize, and manage resources for both planned and unexpected work. Activating Resource Management automatically activates the Project Management plugin if it is not already active. Only upgrade is allowed for this plugin. Activation should be done through PPM Standard plugin.</td>
<td>Inactive</td>
<td>true</td>
<td>• com.snc.schedule_loader&lt;br&gt;• com.snc.process_flow_formatter&lt;br&gt;• com.snc.cost_management&lt;br&gt;• com.snc.pps_portal_common</td>
</tr>
<tr>
<td>Resource Matching Engine</td>
<td>com.snc.matching_rule</td>
<td>Provides a Resource Matching Engine.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.snc.skills_management&lt;br&gt;• com.snc.agent_schedule</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Responsive Canvas</td>
<td>com.glideapp.canvas</td>
<td>Enables responsive canvas. For dashboards, the responsive canvas dynamically responds to dashboard resizing and enables dragging to place and resize widgets. Easily find and preview widgets that you want to add directly from the canvas.</td>
<td>Active</td>
<td>false</td>
<td>• com.glideapp.home</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.text_search</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.db_images</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.ui.angular</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.ui.ng</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Responsive Dashboards</td>
<td>com.glideapp.dashboards</td>
<td>Easily create, modify, and share dashboards using responsive and dynamic widget layouts.</td>
<td>Active</td>
<td>false</td>
<td>• com.glideapp.canvas</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glideapp.home</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.text_search</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.db_images</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.ui.angular</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.ui.ng</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>REST API Builder Backend</td>
<td>com.glide.rest.api_builder.backend</td>
<td>REST API Builder Framework data model and crud interfaces.</td>
<td>false</td>
<td></td>
<td>com.glide.api_runtime</td>
</tr>
<tr>
<td>(New in Quebec)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>REST API for global text search</td>
<td>com.glide.globalssearch</td>
<td>REST API for global text search.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.rest</td>
</tr>
<tr>
<td>领域中文插件</td>
<td>字段</td>
<td>描述</td>
<td>状态</td>
<td>是否有示例数据</td>
<td>依赖项</td>
</tr>
<tr>
<td>Responsive Canvas</td>
<td>com.glideapp.canvas</td>
<td>启用响应式画布。为仪表板，响应式画布动态响应于仪表板缩放并允许通过拖放放置和重新大小调整控件。轻松查找并预览您想要直接从画布中添加的控件。</td>
<td>活动</td>
<td>false</td>
<td>• com.glideapp.home</td>
</tr>
<tr>
<td>Responsive Dashboards</td>
<td>com.glideapp.dashboards</td>
<td>轻松创建、修改并共享使用响应式和动态控件布局的仪表板。</td>
<td>活动</td>
<td>false</td>
<td>• com.glideapp.canvas</td>
</tr>
<tr>
<td>REST API Builder Backend (New in Quebec)</td>
<td>com.glide.rest.api_builder.backend</td>
<td>REST API Builder框架数据模型和 crud 接口。</td>
<td>false</td>
<td></td>
<td>com.glide.api_runtime</td>
</tr>
<tr>
<td>REST API for global text search</td>
<td>com.glide.globalssearch</td>
<td>REST API for global text search。</td>
<td>活动</td>
<td>false</td>
<td>com.glide.rest</td>
</tr>
<tr>
<td>REST API Trigger Flow Designer (New in Quebec)</td>
<td>com.glide.hub.flow_trigger.rest</td>
<td>为流程设计者提供REST API，允许创建一个REST端点，该端点在请求时触发流程。</td>
<td>false</td>
<td>• com.glide.hub.flow_trigger</td>
<td>• com.glide.api_runtime</td>
</tr>
<tr>
<td>REST API Provider</td>
<td>com.glide.rest</td>
<td>提供REST API框架来支持RESTful服务。</td>
<td>活动</td>
<td>false</td>
<td>• com.glide.ui.angular</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>------------------------------------------------------</td>
</tr>
<tr>
<td>Restore Deleted Records</td>
<td>com.snc.undelete</td>
<td>Restores deleted records from audited tables and references to those records. Also restores any records that were deleted as a result of a cascade delete rule.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Role Delegation</td>
<td>com.snc.role_delegation</td>
<td>Allows an administrator to designate role delegators, who can delegate any role they have to members of their group.</td>
<td>Active</td>
<td>false</td>
<td>com.glideapp.workflow</td>
</tr>
<tr>
<td>Sales Force Automation application template</td>
<td>com.snc.sfa2</td>
<td>Provides tools to manage sales and marketing operations throughout the sales life cycle from lead generation through contract completion.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.process_flow_formatter</td>
</tr>
<tr>
<td>Scenario Planning for PPM</td>
<td>sn_pw_scenario</td>
<td>Scenario Planning is a simple system to create and compare scenarios for a portfolio.</td>
<td>Active</td>
<td>true</td>
<td>com.snc.financial_planning_pmo</td>
</tr>
<tr>
<td>Schema Map v3</td>
<td>com.glide.erd</td>
<td>Displays the details of tables and their relationships in a visual manner, allowing administrators to view and easily access different parts of the database schema.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.diagrammer</td>
</tr>
<tr>
<td>Scoped Analytics Framework</td>
<td>com.glide.scoped_analytics</td>
<td>Framework for Scoped Applications.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Scoped Application Restricted Caller Access</td>
<td>com.glide.scope.access.restrictedCallerAccess</td>
<td>Allows scoped applications to restrict access to public tables and script includes.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Script Execution Context</td>
<td>com.snc.sn_context</td>
<td>Provides virtual closure mechanism.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Script stats</td>
<td>com.glide.stats.script</td>
<td>Script stats.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.stats.script</td>
</tr>
<tr>
<td>Script Templates</td>
<td>com.glide.script.templates</td>
<td>Provides templates for some script fields.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Script Allowlist Manager</td>
<td>com.glide.script.whitelist</td>
<td>Provides temporary support for continued direct invocation of Java Packages, Constructors, and Methods that are added to an allow list.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Scripted REST APIs</td>
<td>com.glide.scripted_rest_services</td>
<td>Provides a framework for building Scripted REST APIs.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Scripted REST APIs - Error types</td>
<td>com.glide.scripted_rest_services</td>
<td>Provides a framework for building Scripted REST APIs.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Scripted REST APIs - Internal</td>
<td>com.glide.scripted_rest_services</td>
<td>Provides a framework for building Scripted REST APIs.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Scrum Program</td>
<td>com.snc.sdlc.scrum_program</td>
<td>Plan and track the work across multiple Scrum teams that are working towards common objectives.</td>
<td>Inactive</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>SCSS Bootstrap Theme</td>
<td>com.glide.ui.scss.bootstrap</td>
<td>Theme assets for Bootstrap using SCSS.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.ui.scss</td>
</tr>
<tr>
<td>SCSS Content Provider</td>
<td>com.glide.ui.scss</td>
<td>SCSS Content Provider.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>SDL Translation Management System Spoke for Localization Framework (New in Quebec)</td>
<td>com.glide.localization_framework</td>
<td>It integrates Localization Framework with the SDL - Translation Management System. To activate this plugin, install the Localization Framework Installer plugin.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.localization_framework</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>SDLC - SCRUM</td>
<td>com.snc.sdlc.scrum</td>
<td>Adds a release process specific to a Scrum development process. Sits on top of the SDLC application, adding additional agile notions like epics, stories, and sprints.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.sdlc</td>
</tr>
<tr>
<td>Search Suggestions</td>
<td>com.glide.search.suggestions</td>
<td>Provides suggestions when you enter text in a search field.</td>
<td>Active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Dashboard</td>
<td>com.glide.security.dashboard</td>
<td>This plugin activates the Security Dashboard.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.guided_setup</td>
</tr>
</tbody>
</table>
| Security Incident Analytics  | com.snc.security_incident_and_response   | Provides an integration of Security Incident Response with Performance Analytics for trend-based reporting. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.                                                                                                   | Inactive | true           | • com.snc.pa  
• com.snc.treemap  
• com.snc.security_incident |
| Security Incident Response   | com.snc.security_incident                | Provides visibility into the state of an organization’s security using many of the same workflow and reporting capabilities ServiceNow is known for. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.                                                                                          | Inactive | true           | • com.snc.service_management.core  
• com.snc.task_outage  
• com.snc.treemap  
• com.snc.secops.orchestration  
• com.snc.security_support.sir  
• com.snc.whttp  
• com.snc.threat |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
</table>
| Security Incident Response Dependencies                                | com.snc.si_dep    | Installs all the dependent plugins required to support the Security Incident Response application.                                           | Active | false          | • com.snc.security_support.core  
• com.snc.security_support.sir  
• com.snc.runbook_automation.runtime  
• com.snc.task_outage  
• com.snc.treemap  
• com.snc.whtp  
• com.glide.scope.access.restricted_caller  
• com.sn_dependentclient                                                                 |
<p>| Security Incident Response Mobile                                     | com.sn_sir_mobile | As a security operations center (SOC) manager or a user with the Now Platform security analyst role (sn_si.analyst), you can log in to a Now Platform instance directly from your Android or iOS mobile device. With the Security Incident Response Mobile app, you can view, edit, and assign your most current and critical SIR security incidents and response tasks. Notifications inform you when critical security incidents assigned to you arrive. | Inactive |                | com.glide.sg.agent_native_client                                                                                       |
| Security Incident Response UI                                         | com.app_secops_ui | Provides an enhanced user interface for monitoring and resolving threats to an organization’s security. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.          | Inactive | true           | com.snc.security_incident                                                                                          |</p>
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Integration Framework (Available in the ServiceNow Store)</td>
<td>com.snc.sec.int.framework</td>
<td>Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Security Jump Start (ACL Rules) (Available in the ServiceNow Store)</td>
<td>com.snc.system_security</td>
<td>Adds ACL rules to provide a jump-start on securing many system tables, making it easier for an organization to get into production more quickly.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Security Operations ‘Have I Been Pwned?’ Integration (Available in the ServiceNow Store)</td>
<td>com.snc.secops.pwned</td>
<td>Provides the ability to submit Whois lookups on domain names and URLs to obtain context on URL observables, and to make better determination on threats. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.threat, com.snc.security_incident</td>
</tr>
<tr>
<td>Security Operations ArcSight Logger Integration (Available in the ServiceNow Store)</td>
<td>com.snc.secops.arcsight.logger</td>
<td>Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.security_incident</td>
</tr>
<tr>
<td>Security Operations Carbon Black Integration (Available in the ServiceNow Store)</td>
<td>com.snc.secops.carbonblack</td>
<td>Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.secops.orchestration, com.snc.security_incident</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
<td>----------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>Security Operations CrowdStrike Host Integration (Available in the ServiceNow Store)</td>
<td>com.snc.secops.crowdstrike.host</td>
<td>Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.security_incident</td>
</tr>
<tr>
<td>Security Operations CrowdStrike Intelligence Integration (Available in the ServiceNow Store)</td>
<td>com.snc.secops.crowdstrike.intelligence</td>
<td>Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.threat com.snc.threat.intelligence</td>
</tr>
<tr>
<td>Security Operations Elasticsearch Integration (Available in the ServiceNow Store)</td>
<td>com.snc.secops.elasticsearch</td>
<td>Searches your Elasticsearch logs and adds relevant sighting information to your security incidents. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.security_incident</td>
</tr>
<tr>
<td>Security Operations McAfee ESM Integration (Available in the ServiceNow Store)</td>
<td>com.snc.secops.mcafee.esm</td>
<td>Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.security_incident</td>
</tr>
<tr>
<td>Security Operations Microsoft Exchange Integration (Available in the ServiceNow Store)</td>
<td>com.snc.secops.ms-exchange</td>
<td>Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.security_incident</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------------</td>
<td>--------------------------------------------------</td>
</tr>
</tbody>
</table>
| Security Operations Palo Alto Networks - AutoFocus (Available in the ServiceNow Store) | com.snc.secops.paloalto.autofocus        | Provides the ability to integrate the ServiceNow Security Incident Response application with the Palo Alto Networks AutoFocus. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details. | Inactive | false          | • com.snc.security_incident_response  
• com.snc.secops.orchestration                                           |
| Security Operations Palo Alto Networks - Firewall (Available in the ServiceNow Store) | com.snc.secops.paloalto                 | Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details. | Inactive | false          | • com.snc.secops.orchestration  
• com.snc.security_incident_response                                    |
| Security Operations Palo Alto Networks - WildFire (Available in the ServiceNow Store) | com.snc.secops.paloalto.wildfire         | Provides the ability to integrate the ServiceNow Security Incident Response application with the Palo Alto Networks WildFire application. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details. | Inactive | false          | • com.snc.security_incident_response  
• com.snc.secops.orchestration                                           |
<p>| Security Operations Splunk ES Event Ingestion Integration (Available in the ServiceNow Store) | com.snc.secops.splunkes                 | This is the Splunk Enterprise Security Integration for Security Incident Response. | Inactive | false          |                                                  |</p>
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Operations QRadar SIEM Integration (Available in the ServiceNow Store)</td>
<td>com.snc.secops.qradar.siem</td>
<td>Provides the ability to integrate the ServiceNow Security Incident Response application with QRadar SIEM data. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.security_incident</td>
</tr>
<tr>
<td>Security Operations Splunk Integration (Available in the ServiceNow Store)</td>
<td>com.snc.secops.splunk</td>
<td>Searches your Splunk logs and adds relevant sighting information to your security incidents. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.security_incident</td>
</tr>
<tr>
<td>Security Operations Spoke (Available in the ServiceNow Store)</td>
<td>com.snc.secops.spoke</td>
<td>Provides the ability to use Security Operations flows and actions. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.snc.security_incident&lt;br&gt;• com.glide.hub</td>
</tr>
<tr>
<td>Security Operations Tanium Integration (Available in the ServiceNow Store)</td>
<td>com.snc.secops.tanium</td>
<td>Provides the ability to integrate the ServiceNow Security Incident Response application with Tanium data. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.snc.security_incident&lt;br&gt;• com.snc.secops.orchestration</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>---------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>Security Operations WHOIS Integration (Available in the ServiceNow Store)</td>
<td>com.snc.secops.whois</td>
<td>Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.threat</td>
</tr>
<tr>
<td>Security Support Common (Available in the ServiceNow Store)</td>
<td>com.snc.security_support.common</td>
<td>Provides common functionality for use across the various security applications, such as Security Incident Response. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.security_support.core</td>
</tr>
</tbody>
</table>
| Security Support Orchestration                   | com.snc.secops.orchestration | Provides an integration of Security Operations with Orchestration to allow the facilitation of workflow activities within Security Incident Response, Threat Intelligence, or Vulnerability Response. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details. | Inactive | false          | • com.snc.runbook_automation.runtime     
<p>|                                                |                     |                                                                              |        |                | • com.snc.security_support.common       |
| Self-Service Analytics Core                      | com.snc.self_service_analytics | Provides the self-service analytics framework for configuring deflection contexts and activity patterns to collect the case reduction (deflection) metrics. | Active  | false          | com.snc.activity_subscriptions          |</p>
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-Service Analytics for Customer Service</td>
<td>com.snc.pa.self_service_analytics</td>
<td>Tracks case reduction (deflection) metrics and self-service KPIs using performance analytics dashboards. Activation of this plugin on production instances may require a separate Performance Analytics license. Contact ServiceNow for details.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.pa, com.snc.core.automation.connection_credential, com.snc.pa.self_service_analytics, com.snc.self_service_analytics_core</td>
</tr>
<tr>
<td>Self-Service Analytics PA</td>
<td>com.snc.pa.self_service_analytics</td>
<td>Enables users to define and track key performance indicators (KPIs) to measure the effectiveness of self-service channels such as knowledge, community, virtual agent, and service catalog. Activation of this plugin on production instances may require a separate Performance Analytics license. Contact ServiceNow for details.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.pa</td>
</tr>
<tr>
<td>Self Service Password Reset</td>
<td>com.snc.password_reset</td>
<td>Allows locally authenticated users to request a temporary password if they forget their current password.</td>
<td>Active</td>
<td>false</td>
<td>com.glideapp.password_reset</td>
</tr>
<tr>
<td>Self-Service Portal for Analytics</td>
<td>com.snc.pa.bi_service</td>
<td>Self-Service Portal for Analytics - Allows users to request services related to dashboard access.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.pa</td>
</tr>
<tr>
<td>Sentiment Analysis</td>
<td>com.snc.sentiment_analysis</td>
<td>This plugin is used for Sentiment Analysis</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.core.automation.connection_credential</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
</table>
| Server-side JavaScript Debugger | com.glide.debugger | Allows application developers and administrators to efficiently debug scripts that drive the applications they develop and support. | Active | false | • com.glide.ui.angular  
• com.glide.ui.zepto  
• com.glide.ui.font_icons |
| Service Catalog - ATF Tests | com.glideapp.servicecatalog.atf.test | Provides Service Catalog ATF Tests | Active | true |  |
| Service Catalog - Channel Source Analytics (New in Quebec) | com.glideapp.servicecatalog.analytics | Enables the channel source analytics for Catalog Items. | Active | false | com.glideapp.servicecatalog |
| Service Catalog - Domain Separation | com.glideapp.servicecatalog.domain_separation | Enables separation providers to separate catalog items for different domains |  |  |  |
| Service Catalog - Workspace | com.glideapp.servicecatalog.workspace |  | false |  |  |
| Service Catalog Builder (New in Quebec) | com.glideapp.servicecatalog.catalog_builder | Catalog builder for easy creation and maintenance of catalog items. Installation of this plugin allows creation and editing of catalog items as draft and each change needs to be published. | Active | true | • com.glideapp.servicecatalog.platform  
• com.glideapp.servicecatalog.composite_record_producer  
• com.glideapp.servicecatalog.wizard  
• com.glideapp.servicecatalog.catalog_template  
• com.glideapp.servicecatalog.catalog_builder_experience |
| Service Catalog Builder Experience (New in Quebec) | com.glideapp.servicecatalog.catalog_builder_experience | This plugin offers catalog builder experience in UXF. | false |  | • com.sn_canvas_blank  
• com.sn_canvas_chrome |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Catalog Builder internal components (New in Quebec)</td>
<td>com.glideapp.servicecatalog.builder.internal_components</td>
<td>Internal components that make up Catalog Builder. Install this plugin to edit catalog builder experience.</td>
<td>false</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Catalog CMS Extension</td>
<td>com.glideapp.servicecatalog.cms</td>
<td>Provides the ability to define the catalog experience within CMS.</td>
<td>Active</td>
<td>false</td>
<td>com.glideapp.servicecatalog.platform, com.glide.cms</td>
</tr>
<tr>
<td>Service Catalog Composite Record Producer (New in Quebec)</td>
<td>com.glideapp.servicecatalog.composite_record_producer</td>
<td>Composite Record Producer allows records to be created and edited in multiple related tables without needing scripts.</td>
<td>false</td>
<td>com.glideapp.servicecatalog.platform</td>
<td></td>
</tr>
<tr>
<td>Service Catalog core applications</td>
<td>com.glideapp.servicecatalog.core applications</td>
<td>Allows customers to order predefined, bundled goods and services from your IT organization or other departments.</td>
<td>Active</td>
<td>true</td>
<td>com.glideapp.servicecatalog.platform, com.glideapp.servicecatalog.execution_plan, com.glideapp.servicecatalog.currency</td>
</tr>
<tr>
<td>Service Catalog Macroponent internal components (New in Quebec)</td>
<td>com.glideapp.servicecatalog.macroponent.internal_components</td>
<td>Macroponent internal components</td>
<td>false</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Catalog Manager</td>
<td>com.snc.sc_catalog_manager</td>
<td>Provides utility for managing categories, catalog items, and Knowledge Base links for Service Catalogs.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Service Catalog Mobile Employee</td>
<td>com.glideapp.servicecatalog.employee</td>
<td>This plugin contains the configuration, records and catalog webviews that are used in Mobile Employee Experience native application. Do not activate this plugin directly. Activating com.glide.mobile-employee will activate this plugin for you.</td>
<td>Inactive</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Catalog My Request for Mobile</td>
<td>com.glideapp.servicecatalog.request-filter</td>
<td>This plugin contains the configuration, records that are used in Mobile native application for My Request. Do not activate this plugin directly. Activating com.glide.mobile-employee will activate this plugin for you.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Service Catalog REST API</td>
<td>com.glideapp.servicecatalog.reste</td>
<td>Service Catalog REST API.</td>
<td>Active</td>
<td>false</td>
<td>com.glideapp.servicecatalog.scoped.api</td>
</tr>
<tr>
<td>Service Catalog Scoped API</td>
<td>com.glideapp.servicecatalog.scopedapi</td>
<td>Service Catalog Scoped API to support application creation on Service Catalog platform.</td>
<td>Active</td>
<td>true</td>
<td>com.glideapp.servicecatalog</td>
</tr>
<tr>
<td>Service Catalog Template</td>
<td>com.glideapp.servicecatalog.catalog_template</td>
<td>Framework to create and maintain catalog templates.</td>
<td>false</td>
<td></td>
<td>com.glideapp.servicecatalog.platform</td>
</tr>
<tr>
<td>Service Catalog Wizard</td>
<td>com.glideapp.servicecatalog.wizard</td>
<td>Activating this plugin creates the data model for wizards.</td>
<td>false</td>
<td></td>
<td>com.glideapp.servicecatalog.platform</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Service Creator</td>
<td>com.glide.service_creator</td>
<td>Enables a department to offer custom services through the service catalog, such as the HR department offering tuition reimbursement for further education.</td>
<td>Active</td>
<td>true</td>
<td>• com.glide.ui.ng.cc • com.glideapp.servicecatalog.item_designer</td>
</tr>
<tr>
<td>Service Integration and Management (New in Quebec)</td>
<td>com.snc.siam_core</td>
<td>SIAM Core plugin that provides support for Global scope access, required by applications like VMW and Service Onboarding.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Service Level Management</td>
<td>com.snc.sla</td>
<td>Provides the core SLA functionality. SLA Definitions provide conditions to start, pause, stop, cancel and reset Task SLAs against any Task type. In addition, you can specify a schedule on the definition to define the working hours and also a workflow to run against each Task SLA which is typically used to generate notifications.</td>
<td>Active</td>
<td>true</td>
<td>• com.glideapp.workflow • com.glide.schedules • com.glide.relative_duration</td>
</tr>
<tr>
<td>Service Level Management - Contract Management Integration</td>
<td>com.snc.sla.contract2</td>
<td>Extends the existing SLA functionality, by utilizing a contract as the primary document that houses all appropriate data needed to drive the SLA processing of your task. The attach_sla field is added.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Service Level Management Dashboard</td>
<td>com.snc.sla.overview</td>
<td>This plugin provides the My SLAs Dashboard for Service Level Management.</td>
<td>Active</td>
<td>false</td>
<td>• com.glideapp.canvas</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.sla</td>
</tr>
<tr>
<td>Service Level Management Guided Tour</td>
<td>com.snc.sla.guided_tour</td>
<td>Provides the Guided tour of SLA functionality.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Service Level Management PA Dashboard</td>
<td>com.snc.pa.sla.overview</td>
<td>This plugin provides the SLA Overview (Premium) Dashboard. Activation of this plugin on production instances may require a separate Performance Analytics license. Contact ServiceNow for details.</td>
<td>Active</td>
<td>false</td>
<td>• com.glideapp.canvas</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.pa</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.sla</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.sla.breakdowns</td>
</tr>
<tr>
<td>Service Management Core</td>
<td>com.snc.service_management</td>
<td>Installs the core Service Management items used to allow other service-related plugins to work, such as Field Service, Facilities, HR, Legal, Finance, Marketing, and the custom-app creator.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.snc.automatic_assignment</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.asset_management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.process_flow_formatter</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.state_flows</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.knowledge3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.skills_management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.territory_management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.document_management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.task_activity</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.service_management.geolocation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.service_management.m</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.encryption</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.common_workbench</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.ui.checklist</td>
</tr>
<tr>
<td>Service Management Geolocation</td>
<td>com.snc.service_management</td>
<td>Provides Service Management geolocation capabilities.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.geolocation</td>
</tr>
<tr>
<td>Service Management Geolocation Mobile</td>
<td>com.snc.service_management</td>
<td>Adds a menu in the new mobile UI for Service Management Geolocation.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.glide.ui.m</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.service_management.geolocation</td>
</tr>
<tr>
<td>Service Management Virtual Agent Core</td>
<td>com.glideapp.sm_va_core</td>
<td>Provides core functionality for Service Management Virtual Agent.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------</td>
<td>----------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Service Management Virtual Agent Topic Blocks</td>
<td>com.glideapp.cs.sm_topic_blocks</td>
<td>This plugin contains prebuilt re-usable conversation topic blocks for common actions like ordering from the catalog and searching the knowledge base.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.glide.cs.chatbot • com.snc.contextual_search • com.glideapp.servicecatalog.platform</td>
</tr>
<tr>
<td>Service Modeling</td>
<td>com.snc.cmdb.service.modeling</td>
<td>Core infrastructure for Service Modeling used in Service Mapping and Delivery.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.glide.vars • com.snc.cmdb.enterprise</td>
</tr>
<tr>
<td>Service Portal Analytics</td>
<td>com.glide.service-portal.analytics</td>
<td>User Experience Analytics for Service Portal provides dashboard views for monitoring the key performance indicators (KPIs) of web applications built on Service Portal. You can use these insights to optimize your portal.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.appsee</td>
</tr>
<tr>
<td>Service Portfolio Management Foundation Demo Data (New in Quebec)</td>
<td>com.snc.service_portfolio.demo_data</td>
<td>Adds Demo Data for Service Portfolio Management Foundation and SLA Commitments. If you installed the SPM SLA Commitments plugin before New York, this activates the newer version.</td>
<td>Active</td>
<td>true</td>
<td>• com.snc.service_portfolio • com.snc.service_portfolio.sla_commitment</td>
</tr>
<tr>
<td>ServiceNow Add-Ins for Microsoft Office</td>
<td>com.sn_outlook_addin</td>
<td>Enables users to interact with ServiceNow from within Microsoft Office</td>
<td>Inactive</td>
<td>false</td>
<td>• com.snc.platform.security.oauth • com.glide.ui.vtb • com.glideapp.servicecatalog • com.glide.service-poortal</td>
</tr>
<tr>
<td>ServiceNow Antivirus Program</td>
<td>com.glide.snap</td>
<td>ServiceNow Antivirus Program</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>ServiceNow Certificate Inventory and Management</td>
<td>com.sn_disco_certmgmt</td>
<td>Automatically track certificates, provide awareness of upcoming expirations, and drive the workflow to renew them.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ServiceNow Document Viewer</td>
<td>com.snc.documentviewer</td>
<td>Document viewer is a platform feature that will enable users to view enterprise class documents inline within the platform attachment instead of downloading it to the local device and then opening the documents with a locally installed viewer.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.apppdfgenerator</td>
</tr>
<tr>
<td>ServiceNow Flow Designer - Dynamic Inputs</td>
<td>com.glide.hub.dynamic_inputs</td>
<td>Enable flow designers to configure an action using input values that have been dynamically created. During flow design, when you add an action with dynamic inputs to a flow, it calls a data gathering action to collect data and dynamically shows choices based on that returned data. Use dynamic inputs to look up and display choices dynamically rather than using hard-coded options. For example, you can use a dynamic input to generate choices for a spoke integration.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>----------------------------------------------------</td>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>ServiceNow Flow Designer - Dynamic Outputs</td>
<td>com.glide.hub.dynamic_outputs</td>
<td>Enable flow designers to configure an action using output values that have been dynamically created. During flow design, when you add an action with dynamic outputs to a flow, it calls a data gathering action to create a complex object. Use dynamic outputs to create a complex object with a dynamic structure rather than creating a hardcoded object with a static structure. For example, you can use a dynamic output to generate a complex object for a spoke integration.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>ServiceNow IntegrationHub Action Step - MFT</td>
<td>com.glide.hub.action_step.mft</td>
<td>Provides capabilities to copy directory using the SFTP step.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------</td>
<td>----</td>
<td>-------------</td>
<td>-------</td>
<td>---------------</td>
<td>--------------</td>
</tr>
<tr>
<td>ServiceNow IntegrationHub Action Template - Data Streaming</td>
<td>com.glide.hub.action_type.datastream</td>
<td>Activates Data Stream actions in Flow Designer, enabling you to send REST or SOAP requests from Flow Designer to APIs that return a stream of response data larger than 10 MB. Parse stream data into a series of complex object outputs and use the data pills in other actions in a flow.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.hub.action_step.template</td>
</tr>
<tr>
<td>ServiceNow IntegrationHub Action Step - SFTP</td>
<td>com.glide.hub.action_step.sftp</td>
<td>Provides an SSH File Transfer Protocol step to create a reusable action that can access, transfer, or manage files.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.hub.action_step.template</td>
</tr>
<tr>
<td>ServiceNow IntegrationHub Enterprise Pack Installer</td>
<td>com.glide.hub.integrations.enterprise</td>
<td>Installs IntegrationHub enterprise pack to automate human resources, customer relationship management, enterprise resource planning, and more. Includes IntegrationHub professional pack, Microsoft SCCM spoke, and Data Stream actions.</td>
<td>false</td>
<td></td>
<td>• com.glide.hub.integrations.professional • com.sn.sccm.spoke</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>-------------------------------------------------------------</td>
<td>-----------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>ServiceNow IntegrationHub Professional Pack Installer</td>
<td>com.glide.hub.integrations.professional</td>
<td>IntegrationHub professional pack plugins to automate IT operations. Includes IntegrationHub standard pack, Microsoft AD spoke, Microsoft Azure AD spoke, and SSH and Powershell steps.</td>
<td>false</td>
<td></td>
<td>com.glide.hub.integrations.standard</td>
</tr>
<tr>
<td>ServiceNow IntegrationHub Standard Pack Installer</td>
<td>com.glide.hub.integrations.standard</td>
<td>IntegrationHub standard pack plugins to automate developer operations. Includes IntegrationHub starter pack, and JDBC and XML parser steps.</td>
<td></td>
<td></td>
<td>com.glide.hub.action_step.powershell</td>
</tr>
<tr>
<td>ServiceNow IntegrationHub Starter Pack Installer</td>
<td>com.glide.hub.integrations.starter</td>
<td>IntegrationHub starter pack plugins to build your own integrations. Includes HipChat spoke, Microsoft Teams spoke, Slack spoke, Slack webhooks spoke, cBonding spoke, legacy IntegrationHub usage dashboard, and REST and SOAP steps.</td>
<td></td>
<td></td>
<td>com.sn.ad.spoke</td>
</tr>
<tr>
<td>ServiceNow Language Detection Service Spoke (New in Quebec)</td>
<td>com.glide.language_detection</td>
<td>ServiceNow Language Detection service, it adds ability to detect the language of given text.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.hub</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>.com.glide.hub.integration.runtime</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>ServiceNow Mobile Request - My Request Filter</td>
<td>[com.glideapp.servicecatalog.request-filter]</td>
<td>Plugin contains the configuration and records that are used in the Now Mobile app. Do not activate this plugin directly. Activating com.glide.mobile-employee will activate this plugin for you.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>ServiceNow Subscription Management</td>
<td>com.snc.usage_admin.snc</td>
<td>ServiceNow Subscription Management.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.usage_admin.base</td>
</tr>
<tr>
<td>Service Owner Workspace</td>
<td>com.spm_owner_workspace</td>
<td>Provides a premium Service Portfolio Management experience. Portfolio managers and service owners access an integrated and graphically intuitive user interface to manage and monitor portfolios and services.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.pa.premium com.snc.spm com.snc.spm.spend com.snc.service_workspace</td>
</tr>
<tr>
<td>Service Portal Agent Chat</td>
<td>com.glide.service-portal.agent-chat</td>
<td>This plugin brings Agent Chat to Service Portal.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.cs com.glide.cs.sn-va-web-client-app</td>
</tr>
<tr>
<td>Service Portal - Knowledge Base</td>
<td>com.glide.service-portal.knowledge-base</td>
<td>Knowledge base for SP</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>Service Portal La Jolla Brand Update</td>
<td>com.glide.service-portal.themes.la-jolla</td>
<td>This plugin will update your /sp and /sp_config portals with the ServiceNow La Jolla branding. The logo, favicon, login page background image, hero banner, theme, and widget instance options are updated when the portal record has not been modified. When the portal record is modified no changes are made and an administrator can manually apply changes by downloading the La Jolla images from the db_image table and applying as well as updating the theme setting of the portal record.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.service-portal</td>
</tr>
<tr>
<td>Service Portal - Service Catalog</td>
<td>com.glide.service-portal.service-catalog</td>
<td>Enables Service Catalog widgets for Service Portal.</td>
<td>Active</td>
<td>false</td>
<td>No</td>
</tr>
<tr>
<td>Service Portal - Service Catalog v2</td>
<td>com.glideapp.servicecatalog</td>
<td>Enables Service Catalog widgets for Service Portal.</td>
<td>Active</td>
<td>false</td>
<td>No</td>
</tr>
<tr>
<td>Service Organization</td>
<td>com.snc.service_organization</td>
<td>This plugin provides the base framework to support any internal or external entity involved in the customer service value chain. E.g. Branches, Stores, Franchises, Institutions.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>----------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>Service Portal - Service Status</td>
<td>com.glide.service-portal.service-status</td>
<td>Service Status gives information on current, planned, and historical outages for Business Services so they do not have to call your Service Desk. Loading demo data randomly generates 90 days of outages for 19 demo data Business Services.</td>
<td>Active</td>
<td>true</td>
<td>com.glide.service-portal</td>
</tr>
<tr>
<td>Service Portal Announcement</td>
<td>com.glide.service-portal.announcements</td>
<td>Enables administrators to broadcast announcements to Service Portal users.</td>
<td>Active</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>Service Portal for Enterprise Service Management</td>
<td>com.glide.service-portal.esm</td>
<td>Provides a default service portal with easy configuration and designer. End-user resources include Knowledge Base, Service Catalog, and Services Status.</td>
<td>Active</td>
<td>true</td>
<td>• com.glide.service-portal</td>
</tr>
<tr>
<td>• com.glide.service-portal.service-status</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.service-portal.sqanda</td>
</tr>
<tr>
<td>• com.glide.service-portal.sqanda</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Portal La Jolla Brand Update</td>
<td>com.glide.service-portal.themes.la-jolla</td>
<td>This plugin updates your /sp and /sp_config portals with the ServiceNow La Jolla branding. If the portal record has not been modified, the logo, favicon, login page background image, hero banner, theme, and widget instance options are updated.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Service Portal Surveys</td>
<td>com.glide.service-portal.survey</td>
<td>Service Portal Surveys and Assessments.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Service Portal User Criteria Support</td>
<td>com.glide.service-portal.user-criteria</td>
<td>Enables Service Portal User Criteria support. Installing this plugin will create new user criteria records for each of your widgets and pages that already have role-based permissions on them.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.glide.service-portal• com.glideapp.user_criteria</td>
</tr>
<tr>
<td>Service Portfolio Management Foundation</td>
<td>com.snc.service_portfolio</td>
<td>Allows an organization to document the business services it provides using a standardized, structured format. Performance against availability commitments is calculated and can be displayed in a homepage.</td>
<td>Inactive</td>
<td>true</td>
<td>• com.snc.service_portfolio_core• com.glideapp.servicecatalog• com.glideapp.summary_report_engine</td>
</tr>
<tr>
<td>Service Portfolio Management Core</td>
<td>com.snc.service_portfolio_core</td>
<td>This plugin contains core functionality for Service Portfolio Management available out of the box by default.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.cmdb</td>
</tr>
<tr>
<td>Service Portfolio Management Premium</td>
<td>com.snc.spm</td>
<td>Collects service offering metrics and allows for roll-up calculations to parent services and taxonomy nodes for performance scores and other metrics as viewed via the Service Owner Workspace plugin.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.snc.pa.premium• com.snc.service_portfolio• com.snc.service_portfolio.sla_commitment• com.snc.task_outage</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Service Portfolio Management Estimated Spend</td>
<td>com.snc.spm.spend</td>
<td>Collects service offering cost and allows for selection between local model and Financial Management model.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.spm</td>
</tr>
</tbody>
</table>
| Service Portfolio Management SLA Commitments | com.snc.service_portfolio.sla | Allows commitments to be defined by an SLA, so that staff can track how efficiently the service desk meets commitments for a service offering. | Active   | true           | • com.snc.service_portfolio  
<p>|                                           |                        |                                                                             |          |                | • com.snc.sla         |
| Service Workspace                          | com.snc.service_workspace | Service Workspace application.                                                | Inactive | false          | com.workspace_core    |
| SessionDebug                               | com.glide.sessiondebug | Provides SessionDebug statements and filtering.                              | Active   | false          |                      |
| Shift Planning (Maintenance mode only)     | com.sn_shift_planning  | Shift Planning plugin. Plan team schedules, shifts and workflows for managing timeoffs and shift swaps requests. | Active   | false          |                      |
| Shodan Exploit Integration (Available in the ServiceNow Store) | sn_vul_shodan         | Provides the ability to integrate the ServiceNow Vulnerability Response application with the Shodan product. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details. | false    | sn_vul         |</p>
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature Pad</td>
<td>com.snc.signaturepad</td>
<td>Provides a tool to allow a digital signature in a .pdf document. The Human Resources application uses this with various documents. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.db_images</td>
</tr>
<tr>
<td>Skill Determination</td>
<td>com.snc.skill_determination</td>
<td>Automatically determine and assign skills for work items.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.skills_management</td>
</tr>
<tr>
<td>Skills Management</td>
<td>com.snc.skills_management</td>
<td>The Skills Management application enables you to organize skills data of service agents and employees in a centralized location. You can use this data to assign tasks based on skills, analyze skill gaps to identify coaching and training needs, optimize your workforce, create career growth plans, and perform skill-based hiring.</td>
<td>Inactive</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>Skill Recommendation (Maintenance mode only)</td>
<td>com.snc.sre</td>
<td>Skill Recommendation - ML prediction model and workflow to recommend and assign skills to agents</td>
<td>Active</td>
<td>false</td>
<td>com.snc.skills_management, com.glide.platform_ml</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
<td>---------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Skills Library Data for Skills Management</td>
<td>com.snc.skills_management.</td>
<td>Provides a library of skill categories and skills that you can start using for quick on-boarding.</td>
<td>Active</td>
<td>true</td>
<td>com.snc.skills_management</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>SLA Breakdowns</td>
<td>com.snc.sla.breakdowns</td>
<td>Provides the ability to generate breakdown data for each Task SLA record. For example, you can generate breakdown data on the basis of the <strong>Assignment group</strong> and <strong>Assigned to</strong> fields.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.sla</td>
</tr>
</tbody>
</table>

**Note:**
You need to have up-to-date versions of script includes `TaskSLAController` and `RepairTaskSLAController` before activating this plugin to ensure that breakdown data is generated correctly. If you have customized versions of the script includes `TaskSLAController` and `RepairTaskSLAController`, you need to incorporate all customizations into the versions of these files from the most recent upgrade.
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>SLA Timeline</td>
<td>com.snc.sla.timeline</td>
<td>Provides the ability to view an SLA in a timeline.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>SM Planned Maintenance</td>
<td>com.snc.planned_maintenance</td>
<td>Allows setup and configuration for repeating and triggered requests. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.service_management.core</td>
</tr>
<tr>
<td>SMS Preferences</td>
<td>com.snc.sms_pref</td>
<td>Provides ability to set SMS preferences for receiving messages from different providers.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>sn-custom-tinymce-scoped-app</td>
<td>com.sn-custom-tinymce-scoped-app</td>
<td>Scoped app providing custom tinymce build</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>SNC Code Editor</td>
<td>com.glide.snc_code_editor</td>
<td></td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------</td>
<td>----------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| sn-process-automation-designer | com.sn_process_automation_designer | Plugin is the Process Automation Designer application | Active | false | • com.glide.uxbuilder
  • com.devsc_sn_glide_form_controls
  • com.devsc_sn_record_input
  • com.servicenow_now_alert
  • com.servicenow_now_button
  • com.servicenow_now_card
  • com.servicenow_now_dropdown
  • com.servicenow_now_heading
  • com.servicenow_now_icon
  • com.servicenow_now_label_value
  • com.servicenow_now_modal
  • com.servicenow_now_record_list_connected
  • com.servicenow_now_text_link
  • com.servicenow_now_radio_buttons
  • com.servicenow_now_visual_board
  • com.servicenow_sass_generic
  • com.servicenow_sass_global
  • com.servicenow_ui_core
  • com.servicenow_ui_effect_graphql
  • com.servicenow_ui_effect_helpers
  • com.servicenow_ui_effect_http
  • com.servicenow_ui_enzyme_adapter
  • com.servicenow_ui_renderer_snabbdom
  • com.sn_component_error_handler
  • com.sn_pd_picker
  • com.sn_uxpage_presource |
| sn-ui-builder               | com.sn_ui_builder       | UI Builder is an enjoyable, easy to use builder for creating UIs at ServiceNow. | Active | false | • com.glide.uxbuilder
  • com.servicenow_behavior_focus
  • @servicenow/now-alert
  • @servicenow/now-modal
  • @servicenow/now-text-link
  • sn-devx-components
  • com.sn_http_request
  • com.sn_translate
  • sn-ui-builder-components
  • sn-uxf-builder-middleware |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Asset Management Machine Learning Normalization (New in Quebec)</td>
<td>com.sn_sam_ml_normalization</td>
<td>Provides core capabilities to normalize unrecognized discovered software using machine learning. Requires Software Asset Management Professional.</td>
<td>false</td>
<td></td>
<td>• com.snc.samp</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.platform_ml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software Development Lifecycle (SDLC)</td>
<td>com.snc.sdle</td>
<td>Extends the Release Management v2 plugin by adding some new structures to accommodate the software development life cycle. This plugin is designed to accommodate most non-agile development methodologies, including the common waterfall method of development.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.release_management_v2</td>
</tr>
<tr>
<td>Special Handling Notes</td>
<td>com.sn.shn</td>
<td>Special Handling Notes.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Special Handling Notes Demo Data</td>
<td>com.snc.shn_demo</td>
<td>Special Handling Notes application demo data.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.sn.shn</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.customerservice.demo</td>
</tr>
<tr>
<td>State Flows</td>
<td>com.snc.state_flows</td>
<td>Enables advanced users to customize the state flow of any task table that uses states.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>State Transition Models (New in Quebec)</td>
<td>com.snc.itsm.state_transition</td>
<td>State Transition Models allow flexible configuration of state and transition models.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>State Transition Models - Foundation Data</td>
<td>com.snc.itsm.state_transition</td>
<td>Foundation data for State Transition Models, including State transition conditions.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.itsm.state_transition_model</td>
</tr>
<tr>
<td>Strategic Spend Tracking for PPM</td>
<td>sn_ppm_sst</td>
<td>Evaluate strategic value of your projects and demands.</td>
<td>Active</td>
<td>True</td>
<td>com.snc.financial_planning_pmo</td>
</tr>
<tr>
<td>Studio</td>
<td>com.glide.dev-studio</td>
<td>Allows developers to add and update application files.</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.code-search</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.financial_planning_pmo</td>
</tr>
<tr>
<td>Subscription Administration Base</td>
<td>com.snc.usage_admin.base</td>
<td>Subscription Administration Base.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.subscription_framework</td>
</tr>
<tr>
<td>Subscription Based Notifications</td>
<td>com.glide.notification</td>
<td>Allows users to subscribe to notifications on a task or CI without being on the watchlist or being one of the assigned users.</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.ui_policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.email_notification_preview</td>
</tr>
<tr>
<td>Subscription Based Notifications 2.0</td>
<td>com.glide.notification.subscription</td>
<td>The notification subscription model - improved and simplified.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.notification</td>
</tr>
<tr>
<td>Subscription Management and Enforcement Framework</td>
<td>com.glide.subscription_framework</td>
<td>Subscription Management and Enforcement Framework.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.usageanalytics</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Subscriptions and Activity Feed Framework</td>
<td>com.snc.activity_subscriptions</td>
<td>This plugin provides a generic set of artifacts to handle subscriptions for any defined subscribable object. Any entity can be defined as a subscribable object and a set of subscribers can subscribe to the objects. When an event occurs related to the subscribable object, activities can be tracked and subscribers can be notified.</td>
<td>Inactive</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>Success Indicators</td>
<td>com.snc.vendor.insights</td>
<td>Leverages odds ratio and ML capabilities for apps like Vendor Manager Workspace, etc.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Survey Designer</td>
<td>com.glide.survey_designer</td>
<td>Activates survey designer that is a drag-and-drop interface to create surveys.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.assessment_designer.common</td>
</tr>
<tr>
<td>Survey Management</td>
<td>com.glideapp.survey</td>
<td>Provides Sentiment Analysis capability to determine whether user responses are considered positive, negative or neutral.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Syntax Editor</td>
<td>com.glide.syntax_editor</td>
<td></td>
<td>Active</td>
<td>false</td>
<td>com.glide.snc_code_editor</td>
</tr>
<tr>
<td>System Applications Core</td>
<td>com.snc.apps</td>
<td>Core applications development.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.apps_picker</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------</td>
<td>---------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>System Applications Support</td>
<td>com.snc.apps_complete</td>
<td>Provides support for creating and managing applications.</td>
<td>Active</td>
<td>false</td>
<td>• com.snc.apps&lt;br&gt;• com.snc.apps_picker&lt;br&gt;• com.snc.apps_access&lt;br&gt;• com.snc.apps_file&lt;br&gt;• com.snc.apps_hub&lt;br&gt;• com.snc.apps_legacy&lt;br&gt;• com.snc.metadata&lt;br&gt;• com.snc.metadata_tree&lt;br&gt;• com.snc.apps_creator&lt;br&gt;• com.glide.sessiondebug&lt;br&gt;• com.glide.autorecovery&lt;br&gt;• com.glide.transaction_scope&lt;br&gt;• com.glide.ui.mergetool&lt;br&gt;• com.glide.ui.relationship_layout</td>
</tr>
<tr>
<td>System Import Sets</td>
<td>com.glide.system_import_set</td>
<td>Provides the functionality for import sets.</td>
<td>Active</td>
<td>false</td>
<td>• com.snc.automation&lt;br&gt;• com.glide.ui_policy&lt;br&gt;• com.glide.system_import_data_source</td>
</tr>
<tr>
<td>System Update Set Picker</td>
<td>com.glide.system_update_set</td>
<td><strong>Disabled</strong> users to choose an update set for tracking customizations.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.system_update_set</td>
</tr>
<tr>
<td>System Update Sets (viewer)</td>
<td>com.glide.local_update_set</td>
<td>Provides useful descriptions for update set entries and supports viewing contents of update sets.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>System Update Sets (with remote update set support)</td>
<td>com.glide.system_update_set</td>
<td>Facilitates moving customizations between systems. Supports viewing contents of update sets.</td>
<td>Active</td>
<td>false</td>
<td>• com.snc.apps_hub&lt;br&gt;• com.glide.system_update_set_picker&lt;br&gt;• com.glide.system_update_set_preview</td>
</tr>
<tr>
<td>System Update Sets Preview</td>
<td>com.glide.system_update_set</td>
<td><strong>Disabled</strong> users to preview the changes that are performed by an update set and predict whether there will be any collisions in attempting to apply the update set.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.system_update_set</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| System Web Services             | com.glide.web_service_application| Provides a series of web service import sets.                               | Active| false          | • com.glide.web_service_provider  
|                                 |                                  |                                                                             |       |                | • com.glide.web_service_import_sets  
|                                 |                                  |                                                                             |       |                | • com.snc.web_service_import_set_tables                                    |
| Tablet Device Support - iPad    | com.glide.ui.tablet              | Provides a UI supporting nearly full-product functionality on the Apple iPad.| Inactive| false          | • com.glide.context_help  
| with iOS 6+                      |                                  |                                                                             |       |                | • com.glide.ui.font_icons  
<p>|                                 |                                  |                                                                             |       |                | • com.glide.ui.tablet.theme                                               |
| Tag Data Governance(Maintenance mode only) | com.sn_itom_tag | This store application(beta) provides customers a way to get their cloud resources tagged per enterprise norms, in order to improve return on investments. | Active| false          |                                                                             |
| Targeted Communications          | com.sn_publications              | Provides a way to publish and send out newsletter like articles to targeted internal/external customers. | Inactive| true           | com.snc.cs_base                                                             |
| Targeted Communications Demo Data | com.snc.publications_demo       | Targeted Communications application demo data.                             | Inactive| true           | com.snc_publications                                                        |
| Task Activities                  | com.snc.task_activity            | Enables support for activities on task tables.                             | Inactive| false          |                                                                             |
| Task-Outage Relationship         | com.snc.task_outage              | Allows users to create an outage from an incident and a problem form. Incidents and problems have many to many relationship with outages. For new instances from Jakarta only, this feature is also available on the Change form. | Inactive| false          |                                                                             |</p>
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
</table>
| Team Development          | com.snc.apps_hub  | Supports parallel development on multiple, non-production ServiceNow instances by providing branching operations, the ability to compare a development instance to other development instances, and a central dashboard for all team development activities. | Active| false          | • com.snc.apps  
  • com.glide.ui.angular                          |
| Team Performance          | com.sn_team_perf   | Team Performance module for Workforce Optimization                                                                                                                                                         | Active| false          | com.snc.wfo                                          |
| Templated Snippets        | com.sn_templated_snip | Activated with Human Resources Scoped App: Core [com.sn_hr_core]. Creates pre-defined and reusable responses that can be added to any table extending the task table including the HR Case table. | Inactive| true          | com.glide.scope.access.restricted_caller           |
| Test Management           | com.snc.test_mgmt | Provides a tool for manual software testing.                                                                                                                                                               | Inactive| true          | com.snc.planned_task_v2                            |
| Test Management 2.0       | com.snc.test_management.2.0 | Enables you to manage testing processes and deliver software products more efficiently, with fewer errors.                                                                                      | Inactive| false          | • com.snc.planned_task_v2  
  • com.snc.sdlc.agile.2.0.common                   |
| Test Migration 2.0 - Data Migration | com.snc.test_migration_v1_v2 | The Test Migration plugin provides functionality for migrating Test Case, Test and Test Suite to Test Management 2.0 Test version, Test Step and Test Set.                                                   | Active| false          | • com.snc.test_mgmt  
  • com.snc.test_management.2.0                      |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text Index Attachments</td>
<td>com.glide.text_indexAttachments</td>
<td>Text Index Attachments - natural language search using Lucene syntax.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.text_index</td>
</tr>
<tr>
<td>Text Search</td>
<td>com.glide.text_search</td>
<td>Text Searching across multiple tables.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.text_index</td>
</tr>
<tr>
<td>Threat Core</td>
<td>com.snc.threat</td>
<td>Integrates Threat Intelligence with other Security Operations applications. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.secops.orchestration</td>
</tr>
<tr>
<td>Threat Intelligence</td>
<td>com.snc.threat.intelligence</td>
<td>Provides a point of reference for your company's Structured Threat Information Expression (STIX) data. Included in Threat Intelligence is the Security Case Management application. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.threat</td>
</tr>
<tr>
<td>Threat Intelligence Recorded Future</td>
<td>com.snc.threat.recordedfuture</td>
<td>Enriches security incidents with valuable threat data. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.threat.intelligence</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Time card management</td>
<td>com.snc.time_card</td>
<td>Works with the Task table to record time worked on projects, incidents, problems, and change requests. Task assignees can record time worked in the <strong>Time worked</strong> field on a task record or enter hours directly onto a time card.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.time_card_portal</td>
</tr>
<tr>
<td>Time Recording for Customer Service</td>
<td>com.snc.csm_time_recording</td>
<td>Enables customer service agents to record time on cases, case tasks, and other activities. Recording time automatically generates time cards and time sheets for approval by customer service managers.</td>
<td>Inactive</td>
<td>false</td>
<td>• com.snc.wm_time_recording</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.sn_customerservice</td>
</tr>
<tr>
<td>Time Recording for Field Service</td>
<td>com.snc.time_recording_fsm</td>
<td>Extends the functionality of the Time Card Management and Cost Management applications to Field Service Management. Field service agents record time worked on tasks and other activities. These time worked entries automatically create time cards and weekly time sheets. Managers can review and approve time sheets as well as view and create labor rate cards.</td>
<td>Inactive</td>
<td>true</td>
<td>• com.snc.work_management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.wm_time_recording</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>-------------------------------------------------------------------</td>
</tr>
<tr>
<td>Timeline Visualization</td>
<td>com.snc.timeline_visualization</td>
<td>Enables graphical representation of activities over time to provide a high-level view of strategic and operational activities in your organization such as incidents, problems, changes, and projects. A base system visualization provided by this plugin is the CIO Roadmap. This roadmap shows projects grouped by portfolios. Organization leaders can use the CIO roadmap to monitor and evaluate the status of current and upcoming projects.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.project_management_v3</td>
</tr>
<tr>
<td>Tiny URL Support</td>
<td>com.glide.tiny_url</td>
<td>Enables support for generating shortened URLs to eliminate problems with very long URLs in Internet Explorer. New properties will be added to the System properties page.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>TinyMCE HTML Field Editor</td>
<td>com.glide.editor.tinymce</td>
<td>Enables users to edit HTML fields with the TinyMCE editor instead of the legacy (htmlArea) editor.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Transaction Design Scope</td>
<td>com.glide.transaction_scope</td>
<td>Handles transaction design scope management.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Transaction Quotas</td>
<td>com.glide.quota</td>
<td>Allows definition of quota policies for different types of transactions. A transaction quota cancels any transaction in violation of the policy and notifies the user of the cancellation.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Transform Definitions</td>
<td>com.glide.transform.definition</td>
<td>Activates transform functions which enables flow designers to transform a data pill or field's data type without writing a script.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.transform</td>
</tr>
<tr>
<td>Transform Service</td>
<td>com.glide.transform</td>
<td>Supports use of Transform APIs associated with the Remote Tables functionality.</td>
<td></td>
<td>false</td>
<td>com.glide.transform</td>
</tr>
<tr>
<td>Transaction stats</td>
<td>com.glide.stats.transaction</td>
<td>Transaction stats.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.stats</td>
</tr>
<tr>
<td>Tree map</td>
<td>com.snc.treemap</td>
<td>Enables support for treemap view on any applications.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.pa</td>
</tr>
<tr>
<td>Trusted Security Circles Client</td>
<td>com.snc.intel_sharing.client</td>
<td>Provides the ability to set up communication channels that connect sets of Trusted Security Circles customers who have some kind of underlying relationship. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.threat</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Trusted Security Circles Client (Advanced)</td>
<td>com.snc.intel_sharing.clnt.ad</td>
<td>Provides the capabilities of the basic level, along with the ability to join any available trusted circle and initiate an unlimited number of threat shares per day. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.intel_sharing.client</td>
</tr>
<tr>
<td>UI 15</td>
<td>com.glide.ui.doctype</td>
<td>Enables UI15, a user interface for modern browsers with refined colors and usability enhancements.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.ui11</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>com.glide.ui.recent_selections</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>com.glide.ui.themes.doctype</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>com.glide.ui.font_icons</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>com.glide.ui.ng</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>com.glide.editor.tinymce</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>com.glide.ui.personalize_form</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>com.glide.ui.overview_help</td>
</tr>
<tr>
<td>UI Common</td>
<td>com.glide.ui.common</td>
<td>Glide UI Common</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.ui.ng</td>
</tr>
<tr>
<td>UI Components</td>
<td>com.glideapp.ui_components</td>
<td>Provides all common angular components for apps.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.ui.angularui</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>com.glide.ui.heisenberg</td>
</tr>
<tr>
<td>UI16</td>
<td>com.glide.ui.ui16</td>
<td>Enables UI16, a user interface that provides an updated look and usability improvements. Notable features include real-time form updates, user presence, a redesigned application navigator with tabs for favorites and history, and enhanced activity streams.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.ui.doctype</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>com.glide.ui.concourse</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>com.glide.ui.form_presence</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>com.glide.ui.snippets</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>Universal Request Integration for Incident management</td>
<td>com.snc.incident.universal_request</td>
<td>This plugin delivers Universal Request Integration for Incident Management. It is a developer plugin.</td>
<td>False</td>
<td>True</td>
<td>com.snc.universal_request</td>
</tr>
<tr>
<td>Universal Request: Advanced Work Assignment</td>
<td>com.snc.universal_request.awa</td>
<td>Enables to use Advanced Work Assignment and automatically assign work items to your agents, based on their availability in the Universal Request application.</td>
<td>False</td>
<td>True</td>
<td>com.snc.universal_request</td>
</tr>
<tr>
<td>Universal Request: NLU Model for Virtual Agent Conversations</td>
<td>com.snc.universal_request.nlu</td>
<td>Allows the use of NLU for virtual agent conversations in Universal Request.</td>
<td>False</td>
<td>True</td>
<td></td>
</tr>
<tr>
<td>Universal Request: Reporting</td>
<td>com.snc.universal_request.reporting</td>
<td>Enables to use reports in Universal Request.</td>
<td>False</td>
<td>True</td>
<td></td>
</tr>
<tr>
<td>Universal Request: Virtual Agent Conversations</td>
<td>com.snc.universal_request.va</td>
<td>Helps to set up and use Virtual Agent in Universal Request.</td>
<td>False</td>
<td>True</td>
<td></td>
</tr>
<tr>
<td>Predictive Intelligence for Universal Request</td>
<td>com.snc.universal_request.ml</td>
<td>Facilitates to use machine-learning solutions in the Universal Request application, if you have the admin role.</td>
<td>False</td>
<td>True</td>
<td>com.snc.universal_request</td>
</tr>
<tr>
<td>Universal Request</td>
<td>com.snc.universal_request</td>
<td>Install this plugin to use the Universal Request application.</td>
<td>False</td>
<td>True</td>
<td></td>
</tr>
<tr>
<td>Update Set Batching</td>
<td>com.glide.system_hierarchy_update_set</td>
<td>Deploy update sets in a group.</td>
<td>Active</td>
<td>False</td>
<td>com.glide.system_update_set</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Upgrade Blame Tool</td>
<td>com.glide.upgrade_blame</td>
<td>Tracks the affected table records touched (insert/update/delete) by the load files during system upgrade, zboot, or plugin activation/upgrade. This plugin adds application modules to allow ServiceNow employees to access the upgrade blame log and to turn on/off the feature. It also adds security access control rules to prevent user from modifying the upgrade blame logs table.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Upgrade Metric</td>
<td>com.glide.upgrade_metric</td>
<td>This plugin uses the Upgrade Metric table to track the changes that take a long time to load during upgrades.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>User Criteria Scoped API</td>
<td>com.glideapp.user_criteria.scoped.api</td>
<td>User Criteria Scoped API to support CRUD operations on User Criteria.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glideapp.user_criteria</td>
</tr>
<tr>
<td>User Guide</td>
<td>com.glide.user_guide</td>
<td>Provides the ability to create end-user help documentation that is specific to the policies and procedures of your organization. A default help page is provided in the base system that displays UI16 help documents for system navigation and other basic operations.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User Experience Analytics</td>
<td>com.glide.appsee</td>
<td>Checks for new web and mobile applications to register and provides users access to the Dashboard.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.serviceproxy</td>
</tr>
<tr>
<td>User Registration Request</td>
<td>com.snc.user_registration</td>
<td>Provides the ability for unregistered users to request access to a ServiceNow instance.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Vendor Manager Workspace</td>
<td>com.snc.vlm.vmw</td>
<td>Access to the Vendor Manager Workspace.</td>
<td>Inactive</td>
<td>false</td>
<td>• Performance Analytics - Premium</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Service Workspace, Vendor Manager Workspace - Core</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Service Owner Workspace, UX Framework</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• GraphQL Plugin</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Interactions Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Agent Workspace - Main Configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Agent Workspace - Ribbon</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Agent Workspace - List</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Agent Workspace - Form</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.agent_workspace.global_search</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.agent_workspace.declarative_actions</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.agent_workspace.highlighted_values</td>
</tr>
<tr>
<td>Vendor Manager Workspace - Core</td>
<td>com.snc.vlm</td>
<td>Configure the Vendor Manager Workspace.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Vendor Performance Management (Planned for depreciation in March 2025 or subscription term end)</td>
<td>com.snc.vendor_performance</td>
<td>Provides capabilities to measure, manage, and track vendor data and compare performance characteristics in unique graphical views.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.assessment_core</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>Vendor Success Indicators (New in Quebec)</td>
<td>com.snc.vendor.insights</td>
<td>Vendor Success Indicators to utilize Odds Ratio and other ML capabilities for Vendor Manager Workspace.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.app.ml.insights</td>
</tr>
</tbody>
</table>
| Vendor Ticketing                            | com.snc.vendor_ticket | Provides expanded functionality to obtain vendor performance data by tracking vendor incidents and SLAs. | Inactive | true           | • com.snc.service_portfolio  
• com.snc.service_portfolio.sla  
• com.snc.task_outage  
• com.snc.vendor_performance |
| Version Management                          | com.snc.version  | Provides the ability to track, compare, and revert to multiple versions of table records. | Active  | false          |                                            |
| Version Support                             | com.glideapp.version | Supports tracking versions of files that are stored in update sets, including the ability to compare and revert to previous versions. | Active  | false          |                                            |
| Virtual Agent Analytics Dashboard           | com.glide.cs.pa | Enables the Virtual Agent out-of-the-box analytics dashboard for monitoring conversations and topic usage, including Live Agent metrics. |        |                |                                            |
| Virtual Agent integration with actionable notifications (New in Quebec) | com.glide.cs.actionable.notification | Enables ServiceNow actionable notifications on Virtual Agent chat channels. | Active  | false          | com.glide.cs.notification                  |
| Virtual Agent integration with notifications | com.glide.cs.notification | Enable ServiceNow notifications on Virtual Agent chat channels. | Inactive | false          | • com.glide.cs  
• com.glide.notification.provider |
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Agent Platform Topics</td>
<td>com.glide.cs.topics</td>
<td>Core conversation topics that support Virtual Agent platform conversation flows.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.cs</td>
</tr>
<tr>
<td>Virtual Agent Platform Topic Blocks</td>
<td>com.glide.cs.topic_blocks</td>
<td>Topic blocks required to support core Virtual Agent platform conversation topics</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.cs</td>
</tr>
<tr>
<td>Virtual Agent Service Portal Widgets</td>
<td>com.glide.va.sp_widgets</td>
<td>Virtual Agent Service Portal Widgets</td>
<td>Inactive</td>
<td>true</td>
<td>• com.glide.service-portal&lt;br&gt;• com.glide.cs&lt;br&gt;• com.glide.cs.sn-va-web-client-app</td>
</tr>
<tr>
<td>Virtual Agent Web Client</td>
<td>com.glide.cs.sn-va-web-client-app</td>
<td>Scoped app for the virtual agent web client.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>VirusTotal Integration</td>
<td>com.snc.threat.virustotal</td>
<td>Enables the VirusTotal scanner in Threat Intelligence. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.threat</td>
</tr>
<tr>
<td>Visual Task Board Flow Designer Spoke</td>
<td>com.glide.ui.vtb.ah</td>
<td>The Visual Task Board (VTB) Spoke for the Flow Designer provides Actions enable process analysts to compose flows that manipulate task boards, cards, board members, and assignees on given tasks without having to write code. The Visual Task Board Plugin (com.glide.ui.vtb.ah) should be installed to use these actions.</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.ui.vtb&lt;br&gt;• com.glide.hub.designer_backend.model</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Visual Task Boards</td>
<td>com.glide.ui.vtb</td>
<td>Allows users to organize, modify, and track progress of multiple tasks from an intuitive, Kanban-inspired interface.</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.ui.ng</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.ui.font_icons</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.task</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.ui.checklist</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.ui.ng.amb</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.ui.ng.filter</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.glide.ui.magellan_navigator_api</td>
</tr>
<tr>
<td>Vulnerability Response</td>
<td>com.snc.vulnerability</td>
<td>Allows security users to compare security data pulled from internal and external sources and, if CIs or software are found to be vulnerable, changes and security incidents can be created using Vulnerability Groups. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>true</td>
<td>• com.snc.sam.core</td>
</tr>
<tr>
<td>(Available in the</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.secops.orchestration</td>
</tr>
<tr>
<td>ServiceNow Store)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• com.snc.security_support.vul</td>
</tr>
<tr>
<td>Vulnerability Response</td>
<td>com.snc.vul_dep</td>
<td>System dependencies required by Vulnerability Response. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>false</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dependencies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability Response</td>
<td>com.snc.vul_mobile</td>
<td>As a remediation owner, you can access the Vulnerability Response (VR) application on your Now Platform instance with your Android or iOS mobile device.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.sg.agent_native_client</td>
</tr>
<tr>
<td>Mobile</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Available in the</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ServiceNow Store)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Walk-up Experience</td>
<td>com.snc.walkup</td>
<td>Enables your IT organization to set up a contact channel to support both online check-in and onsite check-in to a pre-established walk-up service center.</td>
<td>Inactive</td>
<td>true</td>
<td>• com.snc.agent_workspace.itsm • com.glide.awa • com.glide.interaction • com.snc.asset_management • com.glide.service-portal • com.snc.appointment_booking • com.glide.db_audio</td>
</tr>
<tr>
<td>Walk-Up for CSM (Maintenance mode only)</td>
<td>com.snc.walkup_for_csm</td>
<td>Walk-up experience for Customer Service enables in-store support to assist onsite check-ins, managing queues, and customer interactions</td>
<td>Active</td>
<td>false</td>
<td>• com.snc.walkup • com.sn_customerservice</td>
</tr>
<tr>
<td>Web Service Consumer</td>
<td>com.glide.web_service_consumer</td>
<td>Provides a SOAP Message module for developing, prototyping, and saving outbound SOAP messages that can be reused in business rules and scripts.</td>
<td>Active</td>
<td>false</td>
<td>• com.glide.vars • com.glideapp.ecc</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Web Service Import Set Tables | com.snc.web_service_import_set_tables | Complements direct web services and scripted web services in providing a web service interface to import set tables. | Active  | false          | • com.glide.web_service_import_sets  
                           • com.glide.web_service_application |
| Web Service Import Sets | com.glide.web_service_import_sets | Complements direct web services and scripted web services in providing a web service interface to import sets. | Active  | false          | • com.glide.table_editor  
                           • com.glide.web_service_provider |
| Web Service Provider - Common | com.glide.web_service_provider | Provides scripted web service and SOAP message resources. | Active  | false          | • com.glide.vars  
                           • com.glide.system_property_categories  
                           • com.glide.system_import_set |
| Web Service Provider - Custom WSDL | com.glide.static_wsdl | Provides the ability to create a scripted web service to accept any WSDL format. | Inactive| false          | |
| Web Service Provider - Scripted | com.glide.custom_web_service | Enables users to create web services that are not addressed by the system. Allows a user to define input and output parameters and use JavaScript to do everything in between. | Active  | false          | • com.glide.web_service_provider  
                           • com.glide.web_service_consumer |
<p>| WebKit HTML to PDF       | com.snc.whtp      | Enables the instance to use the service WebKit HTML to PDF.                  | Inactive| false          | com.snc.platform.security.oauth |
| WFO Mobile (New in Quebec) | com.snc.wfo.mobile |                                                                               |         |                | |
| Widgets                 | com.snc.app.widgets | Provides widget infrastructure along with Angular UI carousel module.        | Inactive| false          | |</p>
<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workflow Authoring Tools</td>
<td>com.glideapp.workflow.author</td>
<td>Allows you to define and modify workflows by arranging and connecting activities with transitions.</td>
<td>Active</td>
<td>true</td>
<td>com.glideapp.workflow</td>
</tr>
<tr>
<td>Workflow Pause Utility</td>
<td>com.glideapp.workflow.pause</td>
<td>Allows you to pause and resume workflows.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Workflow Runtime Engine</td>
<td>com.glideapp.workflow</td>
<td>Enables the creation of workflows that drive automated processes. This may entail generating tasks based on conditions, running scripts, generating approvals, or other actions. Satisfies the same need as the Execution Plans plugin but with greater control and an easier interface.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.diagrander, com.glide.vars, com.glide.schedules, com.gliderelative_duration, com.glide.web_service_application, com.glide.service_api, com.snc.datastructure, com.glideapp.live_feed</td>
</tr>
<tr>
<td>Workflow/Stage element support</td>
<td>com.glide.stages</td>
<td>Support for Workflow-type elements and stage displays.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Workforce Optimization (Maintenance mode only)</td>
<td>com.snc.wfo</td>
<td>Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------</td>
<td>----</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Workspace Core</td>
<td>com.workspace_core</td>
<td>Core Workspace app for enabling CSM/ITSM agents to provide world-class service at light speed.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.uxbuilder, com.snc.agent_workspace.config, com.snc.agent_workspace_global_search</td>
</tr>
<tr>
<td>XML Parser for ServiceNow IntegrationHub</td>
<td>com.glide.hub.action_step.xmlparser</td>
<td>Activates the XML parser step in Flow Designer, enabling you to identify structured data from an XML payload without having to write script.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.hub.action_step.template</td>
</tr>
</tbody>
</table>
### Find components installed with an application

Activating a plugin installs an application on your instance. Each application consists of components such as tables, user roles, and scheduled jobs. To view all components that are installed with an application, see the Application Files table.

- The application plugin must be activated.
- Roles required: admin or the application admin role

**Note:** The application admin role is only required for applications that use the Application administration feature. For example, Vulnerability Response.

In the Application Files table, look up the components that are installed with the plugin for the application. If the application comprises multiple plugins, look up each plugin individually.

1. In the navigation filter, enter: `sys_metadata.list`
   The list of Application Files records is displayed.
2. Click the personalize list icon
   ![Personalize list icon](image)
   and add the **Package** column to the list.
3. Filter the list with these conditions to show only the components for the plugin:
   ```plaintext
   [Package] [is] [<plugin name>]
   ```
4. In the **Class** column heading, click the menu icon
   ![Menu icon](image)
   and select **Group by Class**.

<table>
<thead>
<tr>
<th>Plugin</th>
<th>ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>XTM Translation Management System Spoke for Localization Framework (New in Quebec)</td>
<td>com.glide.localization_framework.xtm_spoke</td>
<td>Integrates Localization Framework with the XTM - Translation Management System. To activate this plugin, install the Localization Framework Installer plugin.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.localization_framework</td>
</tr>
</tbody>
</table>
5. Select the class of information that you want to view.

For example, click **Class: Business Rule** to view all business rules installed with the application.
Using guided setup

Use guided setup to step through the initial configuration of any product or application that provides a Guided Setup module. Guided setup assists you with planning the roll-out of the product and performing the basic configuration to go live.

Guided setup organizes configuration activities into categories. Each category provides information, such as planning guidance, pre-setup steps, and links to useful help content. Categories also provide a set of links to the pages in your instance where you perform the configuration. The guided setup process keeps track of what you have completed, so you can stop and start again where you left off.

Guided setup home page

The home page for most guided setup modules contains an overview and descriptions of the categories and associated tasks. You can click either the home icon or the Get Started button to open the guided setup steps and begin configuration. Click the home icon on the left to return to this page.
Example layout of the guided setup home page
Guided setup categories page

1. Completion indicator

2. Get Started

3. In progress

4. Not started
The completion indicator shows all progress through guided setup steps at a glance. Each circle represents a category and its status.

- Empty circle: The task is not started.
- Circle with a lock: Feature is not activated. You can look at the setup tasks, but not perform them.
- Partial blue border: The percentage of tasks that are complete.
- Circle with curved arrow: Activity tasks were skipped.
- Green circle with check mark: Activity tasks are completed.

Point your cursor at any circle to see what it represents. The percentage at the top is updated as tasks are completed.

2. Category task completion status

For each category, you can view its completion status, which matches its indicator to the left. You can start or continue working on tasks, or edit the statuses of completed tasks.

3. Category information

The category name and description appear. The description often includes further planning information and links to additional content to help you with configuration.

4. Tasks

Lists the tasks and completion status for each activity. Click a task to go to the tasks for that category (same as clicking an action in the second column).

Use the filter above the task list to display only complete or incomplete tasks, as desired.
Guided setup task page

2 / 5 Tasks completed

Task 1
Completed just now by System Administrator

Task 2
Completed just now by System Administrator

Sub-task 1

Sub-task 2

Task 3
Last visited 1m ago by System Administrator
To perform a task, click the **Configure** button. This button opens the page in your instance where the configuration is completed. Embedded help is often available to assist you. If it does not open automatically, click the (?) icon on the upper right.

Other actions you can take include:

- **Breadcrumb**: Click `<Product> Guided Setup` to go back to the categories page.
- **Assign** (upper right): Provides a way to assign tasks to other administrators. All tasks in the category can be assigned to a single admin or each can be assigned individually. The list only displays users with the admin role. When a task is assigned, the admin receives a notification to the email address in their user file.
- **Accept Best Practices**: Click this action if the link appears. Accepting best practices completes some or all of the tasks for that category.
- **Skip**: Click to skip a task if it does not apply to your business process, or you want to implement the feature later.
- **Add Notes**: Click to comment the task, such as stating how far you got before you had to exit. Notes can help another administrator who continues the work.
- **Mark as Complete**: Click this button when the configuration was completed outside of guided setup. After a task is marked complete, the button changes to **Mark as Incomplete**, allowing you to start the task over.
- **More information**: Click this link to read more about the task. The page refreshes with more informative content to help you with the configuration. To return, click the category name in the breadcrumb.

Some tasks have subtasks, represented by tabs below the task information. Task 2 in the illustration is an example of a task with subtasks.

**Other guided setup features**

**Lock icon**

When it appears in front of an activity, task, or subtask, you cannot access the item. You may need to activate a plugin or complete a prerequisite task to unlock it.

**Unlock by activating plugins**

When a category is locked because the associated plugin is inactive, click the **View Plugins** link to see the details in a pop-up window.

**Action buttons**

After beginning guided setup tasks, **Get Started** buttons are changed to **Continue** buttons. Other action buttons change to prompt you to continue with or edit completed tasks.

**Task status and time stamp messages**

Below each task in a task page is a status message. It indicates when the task was last visited or completed and the user who took the action.

**Using Conversational Interfaces Guided Setup**

Use the Conversational Interfaces Guided Setup to create a personalized setup process for just the conversational interface features you need. The Conversational Interfaces Guided Setup starts with a survey and creates a personalized task list based on your survey responses.

Role required: admin
The system admin role is required to activate the plugins and store applications. However, AWA_admin and VA_admin can complete additional setup tasks for their respective solutions.

1. **Navigate to** Guided Setup > Conversational Interfaces Guided Setup.
   
The Conversational Interfaces Guided Setup screen appears.

   ![Conversational Interfaces Guided Setup screen](image)
2. Select **Get Started**.

The Customize Conversational Interfaces Experience > Get started screen appears.
3. On the Get started screen, select **Configure**.

The Customize Conversational Interfaces Experience screen appears.

Let's walk you through the steps you need to take to get your agents chatting.

Once you select which conversational experiences you want to set up, we'll give you specific tasks to complete your setup. [Learn more](#).

The **Workspace Agent Chat** experience allows live agents to communicate with your customers and is available for all subscriptions. The **Virtual Agent** experience uses automated conversations to quickly help your customers.

Select the conversational experiences from your subscription to get your setup steps.

- [ ] Workspace Agent Chat
- [ ] Virtual Agent for Customer Service Management (CSM)
- [ ] Virtual Agent for HR Service Delivery (HR)
- [ ] Virtual Agent for IT Business Management (ITBM)
- [ ] Virtual Agent for IT Service Management (ITSM)
- [ ] Virtual Agent for Instance Security Center (ISC)
4. Complete the survey to generate your personalized list of setup tasks. Choose from:
   - To generate a personalized list of setup tasks, select the solutions you want to activate and configure from the following options:
     a. Workspace Agent Chat
     b. Virtual Agent for Customer Service Management (CSM)
     c. Virtual Agent for HR Service Delivery (HR)
     d. Virtual Agent for IT Business Management (ITBM)
     e. Virtual Agent for IT Service Management (ITSM)
     f. Virtual Agent for Instance Security Center (ISC)

     The preceding Virtual Agent options include predefined chatbot conversations designed to help your users complete common tasks per workflow. For instance, Virtual Agent for IT Service Management includes conversations to support resetting a password and creating an incident.

     Next, select **See my Steps**.
     - To view the full list of every possible setup task for every solution option, select **Skip and see all steps**. You will have access to configure all solution options in your sub-production environment for testing purposes. However, you may not have access to or activate certain solution options unless you licensed for such options.

     **Note:** Make sure to pay attention to steps with asterisks in the title as well as notes within the steps that explain required plugins and store applications prerequisites.

     To learn more about the general guided setup solution, see **Guided Setup**.

**Domain separation and Guided Setup**

Domain separation is unsupported for Guided Setup. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can control several aspects of this separation, including which users can see and access data.

**Support level: No support**

- The domain field may exist on data tables but there is no business logic to manage the data.
- This level is not considered domain-separated.

For more information, see **Application support for domain separation**.
Available system properties

Some properties are available on a system properties form, but some lesser-used properties are available only from the System Property [sys_properties] table. Sometimes, the property does not exist in a base instance, but can be added if you change the value.

Note: The Instance Security Hardening Settings content contains detailed descriptions, and compliance values, for the security-related system properties and plugins in the. To learn more about each of these properties, see Instance Security Hardening Settings.

cdu.record.watcher.timeout

Maximum waiting period for the Cloud Discovery schedule configuration wizard to stop watching the record watchers while validating account, member account Discovery, and logical database Discovery.

• Type: integer
• Default value: 120,000 milliseconds
• Location: System properties

com.cmdb.baseline.max_changes

Maximum number of changes and relationships for a CI that can appear in the baseline diff for the CI.

• Type: integer
• Default value: 100
• Location: Configuration > CMDB Properties > Baseline Properties

com.glide.attachment.max_size

Sets the maximum file attachment size in megabytes. A blank value in this field allows attachments up to a maximum of 1 KB.

• Type: integer
• Default value: 1024
• Location: System Properties > Security

com.glide.csv.loader.ignore_non_parseable_lines

Enables (true) or disables (false) ignoring one or more lines (rows) in an import set that contains bad data, such as a row that is missing a column of data.

• Type: true | false
• Default value: false
• Location: Add the property to the System Property [sys_properties] table.

com.glide.csv.loader.max_errors_allowed

Sets the maximum number of lines (rows) that an import can ignore before failing. If the import succeeds, the import lists the number of rows ignored due to errors.

• Type: integer
• Default value: 100
• Location: Add the property to the System Property [sys_properties] table.

com.glide.email.max_read

Specifies the maximum number of emails a POP3 reader should process concurrently.
• Type: integer  
• Default value: 20  
• Location: Add the property to the System Property [sys_properties] table.

**com.glide.loader.verify_target_field_size**

Controls whether import set fields can automatically increase in size during an import (true) or not (false). By default, data that exceeds the import field size is truncated. Set this property to true to allow any import set field to increase the column size to match the length of the data.

• Type: true | false  
• Default value: false  
• Location: Add the property to the System Property [sys_properties] table.

**com.glide.soap.include_non_db_fields**

Controls whether non-database fields, such as the sys_tags field, are included in WSDLs and SOAP responses (true) or not (false).

• Type: true | false  
• Default value: false  
• Location: Add the property to the System Property [sys_properties] table.

**com.glide.ssl.read.timeout**

Sets the time-out value in seconds for SSL connections during read operations. Typically, this setting is used as part of LDAPS. If you enter timeout values for both this system property and the LDAP Read timeout field, the lowest timeout value takes precedence.

• Type: integer  
• Default value: 10  
• Location: Add the property to the System Property [sys_properties] table.

**com.glideapp.canvas**

Enables (true) or disables (false) responsive canvas for dashboards. When enabled, all new dashboards use responsive canvas. Non-responsive dashboards are not converted to responsive dashboards.

• Type: true | false  
• Default value: true  
• Location: System Property [sys_properties] table

**com.snc.apps.publish.include_inactive_choices**

Specifies whether choice table selections marked as inactive (sys_choice inactive attribute = true) should be included when publishing an application (true) or not (false).

• Type: true | false  
• Default value: true
• Location: System Property [sys_properties] table

**com.snc.apps.publish.maxrows**
Defines the maximum number of data records to include when publishing an application.
• Type: integer
• Default value: 1,000
• Location: System Property [sys_properties] table

**com.snc.assessment.decision_matrix_filter_max_entries**
Defines the maximum number of items to show for a decision matrix field filter.
• Type: integer
• Default value: 1,000
• Location: System Property [sys_properties] table

**com.snc.assessment.signature_authentication**
Requires authentication for a user signature.
• Type: true | false
• Default value: true
• Location: System Property [sys_properties] table

**com.snc.dd.publish_to_app_repo_enabled**
Enables (true) or disables (false) display of the Publish To App Repo permission in Manage Developers.
• Type: true | false
• Default value: true
• Location: System Property [sys_properties] table

**com.snc.dd.publish_to_app_store_enabled**
Enables (true) or disables (false) display of the Publish To App Store permission in Manage Developers.
• Type: true | false
• Default value: true
• Location: System Property [sys_properties] table

**com.snc.dd.publish_to_update_set_enabled**
Enables (true) or disables (false) display of the Publish To Update Set permission in Manage Developers.
• Type: true | false
• Default value: false
• Location: System Property [sys_properties] table

**com.snc.dd.upgrade_app_enabled**
Enables (true) or disables (false) display of the Update App permission in Manage Developers.
• Type: true | false
• Default value: true
• Location: System Property [sys_properties] table
com.snc.hr.core.impersonateCheck

Allows a user to have identical permissions/access as the person they are impersonating. If **true**, access and restrictions apply when impersonating another user. If **false**, the user has identical permissions/access as the person they are impersonating.

- Type: true | false
- Default value: true
- Location: System Property [sys_properties] table

com.snc.iam.log_level

Logging level for the business rule MapUpstreamImpactedCI. Debug is the most detailed option with full trace of how the Impacted CI List is calculated. Error is the minimal logging option with only severe errors being logged.

- Type: string
- Default value: info
- Possible values: debug, info, error
- Location: System Property [sys_properties] table

com.snc.on_call_rotation.reminders.showtz

Specifies whether to show the user time zone (**true**) or not (**false**).

- Type: true | false
- Default value: false
- Location: Add the property to the System Property [sys_properties] table.

com.snc.pa.activate_kpi_signals

Create this property and set to 'false' to deactivate the KPI Signals feature.

- Type: Boolean true | false
- Default value: Does not exist but is treated as 'true'
- Location: Add the property to the System Property [sys_properties] table.

com.snc.pa.dc.batch_score_insert

When true, Performance Analytics data collection jobs insert indicator scores to the database in batches. When false, indicator scores are inserted one by one. Even when true, batch score insertion is performed only as a fallback when hierarchical data collection (com.snc.pa.dc.hierarchical_collection) has been disabled.

- Type: Boolean true | false
- Default value: true
- Location: System Properties [sys_properties] table

com.snc.pa.dc.flush_snapshot_count

Maximum number of Performance Analytics snapshots to store in the memory during data collection. When this number is reached, the snapshots are offloaded to the database, freeing memory.

- Type: integer
- Default value: 1000
- Location: System Properties [sys_properties] table

com.snc.pa.dc.hierarchical_collection

© 2021 ServiceNow, Inc. All rights reserved. 
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Activates a hierarchical approach to score collection, where Indicator > level 1 breakdown > level 2 breakdown. This approach is more resource efficient than a flat hierarchical approach, which creates redundant objects.

- **Type**: Boolean true | false
- **Default value**: true
- **Location**: System Properties [sys_properties] table

**com.snc.pa.dc.max_breakdown_elements_limit**

Maximum number of breakdown elements for a breakdown to be included in data collection.

- **Type**: integer
- **Default value**: 10000
- **Location**: System Property [sys_properties] table

**com.snc.pa.dc.max_error_count**

Maximum errors that may occur before data collection is stopped.

- **Type**: integer
- **Default value**: 500
- **Location**: System Property [sys_properties] table

**com.snc.pa.dc.max_records**

Maximum number of records that are stored during a data collection.

- **Type**: integer
- **Default value**: 5000
- **Location**: System Property [sys_properties] table

**com.snc.pa.dc.max_row_count_indicator_source**

Maximum number of rows that are allowed to be fetched from an Indicator Source.

- **Type**: integer
- **Default value**: 50000
- **Location**: System Property [sys_properties] table

**com.snc.pa.dc.script_timeout**

Maximum time in seconds that a script is allowed to run during a data collection cycle.

- **Type**: integer
- **Default value**: 30
- **Location**: System Property [sys_properties] table

**com.snc.pa.dc.use_hashcode_for_distinct**

Sets whether Count Distinct aggregations are stored as separate values in memory or as a HashCode. When the value of this property is True, a HashCode is used, which consumes less memory than storing individual values.

- **Type**: Boolean true | false
- **Default value**: true
- **Location**: Add the property to the System Property [sys_properties] table

**com.snc.project.default_schedule**
Stores the sys_id of the default schedule attached to projects.
- Type: string
- Location: System Property [sys_properties] table

**com.snc.project.loglevel**
Automatically resubmits timed-out Ajax requests.
- Type: choice list
- Default value: 0 (debugging disabled)
- Location: System Property [sys_properties] table

**com.snc.project.wbs_gantt**
Automatically resubmits timed-out Ajax requests.
- Type: true | false
- Default value: false
- Location: Project > Administration > Properties

**com.snc.task.associate_ci**
List of all task types where user wants to associate CIs using a List system.
- Type: string
- Default: incident,problem,change_request
- Location: System Property [sys_properties] table

**com.snc.task.refresh_impacted_services**
List of all task types where Refresh Impacted Services UI action is enabled.
- Type: string
- Default value: incident,change_request
- Location: System Property [sys_properties] table

**com.snc.time_card.default_rate**
(Cost Management plugin) Sets a default hourly rate to use if no labor rate cards apply to the user.
- Type: integer
- Default value: 50
- Location: System Property [sys_properties] table

**com.snc.time_worked.update_task_timer**
Enables (true) or disables (false) updating the task timer value based on changes to the task time worked records. Uses the Update task time business rule.
- Type: true | false
- Default value: false
- Location: System Property [sys_properties] table

**csm_auto_account_domain_generation**
When new account in Customer Service application is created, domain is created and placed under TOP domain. If parent field on account form is populated, and new record is inserted, it creates that account as a subdomain of the parent.

- Type: true | false
- Default value: false
- Location: System Property [sys_properties] table

**css.assessment.caption.background.color**

Sets the background color of the caption on assessment and survey questionnaires.

- Type: color
- Default value: #eee
- Location:
  - Assessments > Admin > Assessment Properties
  - Survey Management > Administration > Properties

**css.assessment.caption.font.color**

Sets the font color of the caption text on assessment and survey questionnaires.

- Type: color
- Default value: #ffffff
- Location:
  - Assessments > Admin > Assessment Properties
  - Survey Management > Administration > Properties

**css.assessment.question.header.background.color**

Sets the background color of question headers on assessment and survey questionnaires.

- Type: color
- Default value: #767676
- Location:
  - Assessments > Admin > Assessment Properties
  - Survey Management > Administration > Properties

**css.$nav-highlight-main**

Sets the color for the navigation expanded items highlight background.

- Type: color
- Default Value: #3D4853
- Location: System Property [sys_properties] table

**css.$nav-hr-color**

Sets the color for the navigation separator.

- Type: color
- Default Value: #303A46
- Location: System Property [sys_properties] table
css.$navpage-header-bg
Sets the color for the header background.
  • Type: color
  • Default Value: #303A46
  • Location: System Property [sys_properties] table

css.$navpage-header-color
Sets the color for the banner text.
  • Type: color
  • Default Value: #FFFFFF
  • Location: System Property [sys_properties] table

css.$navpage-nav-bg-sub
Sets the color for the background for navigator and sidebars.
  • Type: color
  • Default Value: #455464
  • Location: System Property [sys_properties] table

css.$navpage-nav-border
Sets the color for the border for UI16.
  • Type: color
  • Default Value: #DDD
  • Location: System Property [sys_properties] table

css.$navpage-nav-color-sub
Sets the color for module text in UI16.
  • Type: color
  • Default Value: #BEC1C6
  • Location: System Property [sys_properties] table

css.$navpage-nav-selected-bg
Sets the color for navigator selected tab background.
  • Type: color
  • Default Value: #4B545F
  • Location: System Property [sys_properties] table

css.$navpage-nav-selected-color
Sets the color for the currently selected navigation tab icon color for UI16.
  • Type: color
  • Default Value: #FFFFFF
  • Location: System Property [sys_properties] table

css.tablet.gradient.start
Start color of the gradient for the tablet UI header.
css.tablet.gradient.end
End color of the gradient for the tablet UI header.

- Type: color
- Default value: #111
- Location: System Properties > Tablet UI Properties

css.tablet.headerfooter.text.color
Color of the text and icons in the tablet UI header and footer.

- Type: color
- Default value: #ffffff
- Location: System Properties > Tablet UI Properties

glide.allow.new.cert_follow_on_task
Allow Desired State audit to create a new follow-on task for the same failure at each audit run.

- Type: true | false
- Default value: true
- Location: System Property [sys_properties] table

glide.amb.session.logout.overlay.style
Specifies a cascading style sheet (css) that defines an overlay. The overlay masks all onscreen data on timeout, and the login screen appears on top of the overlay.
Limited to core Now Platform functions, not applications.

- **Type**: string
  
  - Example: background-color: #000; opacity: 0.5
  
- **Default value**: empty (no overlay)
  
- **Location**: System Property [sys_properties] table

### glide.angular.legacy

When true, enables legacy AngularJS behavior. When false, integrates AngularJS sanitizeUri and $http security patches. If you set this property to false, existing JSONP requests with cross-domain endpoints will fail. You can address this issue in your scripts by doing one of the following:

1. Add the domains of any newly failing requests to the `angular.jsonp.inclusion_list.urls` system property.
2. Opt out of this behavior by changing `angular.jsonp.inclusion_list.enabled` to false.

- **Type**: true | false
  
- **Default value**: true
  
- **Location**: System Property [sys_properties] table

### glide.applications.hub.current

URL of the team development parent instance.

- **Type**: string
  
- **Default value**: none
  
- **Location**: System Property [sys_properties] table

### glide.attachment.extensions

Comma-separated list of file extensions that can be attached. No value means that there are no restrictions.

- **Type**: string
  
- **Default value**: none
  
- **Location**: System Properties > Security

### glide.attachment.role

Comma-separated list of roles that can create attachments.

- **Type**: string
  
- **Default value**: public
  
- **Location**: System Properties > Security

### glide.authenticate.multisso.login_locate.user_field

Identifies a common login identifier.

- **Type**: string
  
- **Default value**: user_name
  
- **Location**: Add the property to the System Property [sys_properties] table.

### glide.authenticate.sso.saml2.require_signed_authnrequest

Enables the Identity Provider Single sign-on service to receive a signed AuthnRequest.

- **Type**: true | false
- Default value: false
- Location: System Property [sys_properties] table

**glide.banner.image.url**

URL used when clicking the banner image.

- Type: string
- Default value: home.do
- Location: System Property [sys_properties] table

**glide.banner.image.url_target**

Target frame used when clicking the banner image. Use gsft_main for the main frame, _top to replace the current browser window, _blank for a new window or tab.

- Type: string
- Default value: gsft_main
- Location: System Property [sys_properties] table

**glide.bsm.color.affect_neighbors**

Color of an affected neighbor node. When a node has a service issue, all nodes that depend on that node are considered affected nodes. In the map, the affected nodes are parents or grandparents of the node with the service issue.

- Type: color
- Default value: Beige
- Location: BSM Map > Map Properties

**glide.bsm.map.style.font_family**

Font family name used in the map text. If you designate a font that is not on the user system, the browser substitutes another font and the text may not render as you expect.

- Type: font name
- Default value: Arial
- Location: BSM Map > Map Properties

**glide.bsm.map.style.font_size**

Font size of the text that appears with a CI node. The default size is magnified for nodes with more connections and reduced for downstream nodes.

- Type: integer
- Default value: 14
- Location: BSM Map > Map Properties

**glide.bsm.map.style.selection_background_color**

Background color of a selected CI node. This color is also used with a node's Highlight Hierarchy option.

- Type: color
- Default value: RoyalBlue
- Location: BSM Map > Map Properties

**glide.bsm.map.style.selection_text_color**
Color of the text that appears under a selected CI node.

- **Type:** color
- **Default value:** White
- **Location:** BSM Map > Map Properties

**glide.bsm.map.style.text_color**

Color of the text that appears under an unselected CI node.

- **Type:** color
- **Default value:** Black
- **Location:** BSM Map > Map Properties

**glide.bsm.max_levels**

Maximum level depth from the root CI that can be initially displayed in business service maps. Level depth is the graph distance between the root CI and a node. This value must be an integer.

- **Type:** integer (1-10)
- **Default value:** 5
- **Location:** BSM Map > Map Properties

**glide.bsm.new_node_color**

Color for nodes that became viewable from the last expand operation.

- **Type:** color
- **Default value:** PaleGreen
- **Location:** BSM Map > Map Properties

**glide.bsm.max_nodes**

Maximum number of downstream nodes to retrieve from the database for a CI. If more nodes exist in the database, they are not displayed in the map.

- **Type:** integer
- **Default value:** 1000
- **Location:** BSM Map > Map Properties

**glide.bsm.refresh_interval**

Seconds between each automatic reloading of troubles and tasks.

- **Type:** integer
- **Default value:** 30
- **Range of possible values:** 1 to 3600
- **Location:** BSM Map > Map Properties

**glide.bsm.task_threshold**

Change the CI glyph color from orange to red when the number of tasks reaches this threshold.

- **Type:** integer
- **Default value:** 3
- **Location:** BSM Map > Map Properties
**glide.bsm.too_many_children**

Maximum number of child nodes to display. Nodes are collapsed for the map to meet this limit.

- Type: integer, valid values 1 or greater
- Default value: 10
- Location: **BSM Map > Map Properties**

**glide.businessrule.async_condition_check**

Specifies whether the instance checks the condition statement of async business rules (the **When** field is set to async) prior to running the business rule. If **true**, the instance evaluates the async business rule conditions a second time before running the rule. If **false** or missing, the instance does not evaluate the conditions a second time.

- Type: true | false
- Default value: false
- Location: **Add the property** to the System Property [sys_properties] table.

**glide.businessrule.callstack**

Specifies whether business rule executions are logged in the daily log when they start and finish (**true**) or are not logged (**false**). Logging is useful for troubleshooting a problem where you must know which business rules are running and in which order.

- Type: true | false
- Default value: false
- Location: **Add the property** to the System Property [sys_properties] table.

**glide.cache.size.service_cache**

- Type: integer
- Default value: 20
- Location: **Add the property** to the System Property [sys_properties] table.

**glide.canvas.grid.widget_render_concurrent_max**

Defines the maximum number of widgets that can render simultaneously on a dashboard. With smaller values, individual widgets load more quickly. With larger values, fewer Ajax requests to the server are needed. Set the value of this property to half of the number of widgets that are visible when your most-used dashboard loads. For example, if six widgets are visible on the dashboard set the value to 3.

**Note:** This system property applies to responsive dashboards only.

Two is the minimum value, and 1 is interpreted as 2. For values of zero or lower, all widgets load simultaneously.

- Type: integer
- Default value: none
- Location: System Property [sys_properties] table

**glide.cmdb.query.batch_time_limit_in_sec**

Time limit (in seconds) for running one batch to get one batch of query results (100 results).

- Type: integer
- Default value: 300
- Location: **Configuration > CMDB Properties > Query Builder Properties**
**glide.cmdb.query.max_results_limit**

Limits the number of results for a scheduled query and in the results section in the Query Builder when you click Load All Results.

- Type: integer
- Default value: 10,000
- Location: Configuration > CMDB Properties > Query Builder Properties

**glide.cmdb.query.non_cmdb.blacklisted_tables**

Exclusion list of non-CMDB tables that appear in the CMDB Query Builder when creating a CMDB query.

- Type: string
- Default value: empty
- Location: Configuration > CMDB Properties > Query Builder Properties

**glide.cmdb.query.query_time_limit_in_sec**

Time limit (in seconds) for running an entire query to get all results.

- Type: integer
- Default value: 1,800
- Location: Configuration > CMDB Properties > Query Builder Properties

**glide.cmdb.statemgmt.max_bulk_count**

Maximum number of CIs that CI Lifecycle Management can process in a bulk update operation.

- Type: integer
- Default value: 1000
- Location: System Property [sys_properties] table

**glide.cmdb.statemgmt.max_lease_expired_days**

Maximum number of days that lease expiration can be set with for CI Actions.

- Type: integer
- Default value: 15
- Location: System Property [sys_properties] table

**glide.cms.dashboards.sharing_with_secure_search**

When enabled, the list of users, user groups, and roles that are visible in the sharing panel is restricted. The restriction is based on the configuration of the sys_user, sys_user_group, and sys_user_role ACLs. For more information, see Access control list rules.

There is a performance penalty associated with enabling this property. Performance degradation may be based on the number and complexity of business rules and ACLs on your instance.

- Type: true | false
- Default value: false
- Location: System Properties > Dashboard Properties

**glide.cms.share_dashboards.role**

When this property is empty, all users can share their own dashboards.
Note: This property does not apply to users with the admin and dashboard_admin roles. Users with these roles can always share any dashboard.

- **Type:** string
- **Default value:** empty
- **Location:** System Properties > Dashboard Properties

**glide.chart.decimal.precision**

Controls the rounding precision of non-currency numeric values displayed on reports. A Decimal Precision value specified in a report’s style options overrides this property. Currency values always have a precision of 2.

- **Type:** integer
- **Default value:** 2
- **Maximum value:** 4
- **Location:** Add the property to the System Property [sys_properties] table.

**glide.chat.invite_fields**

(Chat plugin) Comma-separated list of fields (glide_list or references to sys_user or sys_group) used to generate the invitations when creating a chat room from a task. Users can select a check box for each of the specified fields to invite to the chat room users that are referenced by the fields.

- **Type:** string
- **Default value:** none
- **Location:** Social IT > Chat Administration > Properties

**glide.chat_room.create_roles**

(Chat plugin) Comma-separated list of roles that are allowed to create chat rooms.

- **Type:** string
- **Default value:** none
- **Location:** Social IT > Chat Administration > Properties

**glide.chat.show_emoticons**

(Chat plugin) Enables (true) or disables (false) rendering text emoticons as images.

- **Type:** true | false
- **Default value:** true
- **Location:** Social IT > Chat Administration > Properties

**glide.class.downgrade.enabled**

Flag for allowing class downgrade during identification and reconciliation.

- **Type:** true | false
- **Default value:** true
- **Location:** System Properties [sys_properties] table

**glide.class.switch.enabled**

Flag for allowing class switching during identification and reconciliation.

- **Type:** true | false
- **Default value:** true
gslide.class.upgrade.enabled
Flag for allowing class update during identification and reconciliation.
• Type: true | false
• Default value: true
• Location: System Properties [sys_properties] table

gslide.cmdb.health.metricProcessor.maxRunningTime
Max time in minutes for which individual metric processor runs in each scheduled cycle.
• Type: integer
• Default value: 120
• Location: Navigate to Configuration > Health Preference, and then click System Properties in the right hand-side navigator.

gslide.cmdb.health.src.cmdb_health_audit_only
When set to true, disables health results from sources other than CMDB Health audit (such as cloud discovery). Only results generated by CMDB Health audit appear in the CMDB dashboard.
For example, by default, if a CI is determined to be stale by Discovery, then that CI appears as stale in the CMDB dashboard even though CMDB Health audit did not determine that CI to be stale. To disable these stale CI health results, set the property to true.
• Type: true | false
• Default value: false
• Location: System Property [sys_properties] table

gslide.cmdb.health.staleness_exclude_dependent_cis
Exclude dependent CIs for the staleness CMDB Health metric.
When enabled, dependent CIs are not checked for staleness, regardless of any staleness or inclusion rules that are defined for the respective CI types.
• Type: true | false
• Default value: false
• Location: System Property [sys_properties] table

gslide.cmdb.logger.source.identification_engine
Enable and configure what type of details the system logs when using IRE outside the scope of identification simulation. For example, when using an API, ECC queue or scheduled jobs.
• Type: string
• Default value: info, warn, error, debug, or debugVerbose
• Location: Add the property to the System Property [sys_properties] table.

gslide.cmdb.logger.use_syslog.CMDBHealth
A comma-separated list that controls the level of logging of CMDB Health jobs. Logging creates entries in the system logs to capture messages generated by the health auditing process each time they run. This logging helps debugging if there is a failure.
• Type: string
• Default value: error
• Location: System Property [sys_properties] table

**glide.cmdb_model.display_name.shorten**

If `true`, generates shorter display names for product models if the name of the product model contains the manufacturer name.

• Type: `true` | `false`
• Default value: `false`
• Location: System Property [sys_properties] table

**glide.cookies.http_only**

Enables (`true`) or disables (`false`) the generation of HTTP-only cookies. Set this property to `false` to use Approval with E-Signature.

• Type: `true` | `false`
• Default value: `true`
• Location: System Property [sys_properties] table

**glide.cost_mgmt.calc_actual_cost**

(Cost Management plugin) When an expense line is created for any task with a Type of `Planned task`, sums all task expense lines and adds the total to the `Work cost` field on the task record.

• Type: `true` | `false`
• Default value: `true`
• Location: System Property [sys_properties] table

**glide.cost_mgmt.debug**

(Cost Management plugin) Enables debugging of cost management processing. All logging events are recorded in the Financial Management Log [fm_log] table.

**Note:** This feature can generate a large number of log records. Enable the feature only during initial testing or when troubleshooting.

• Type: `true` | `false`
• Default value: `false`
• Location: System Property [sys_properties] table

**glide.cost_mgmt.process_task_cis**

(Cost Management plugin) Creates expense lines affected configuration items when creating a task expense line.

• Type: `true` | `false`
• Default value: `false`
• Location: System Property [sys_properties] table

**glide.cost_mgmt.service_allocation.method**

(Cost Management plugin) Defines whether business service to cost center allocation costs should be calculated based on total units or allocated units.

For example, if the service supports 100 units but only has 50 units allocated, and cost center ABC is allocated 25 units. Using the **All units** method results in an allocation cost of 25/100, or 25% of the total cost of the service. In
In this case, we track unallocated costs separately. Using **Allocation units** method results in an allocation cost of 25/50, or 50% of the total cost of the service. In this case, all costs are allocated (recovered).

- **Type:** choice list
- **Default value:** all_units
- **Location:** System Property [sys_properties] table

**glide.csv.export.line_break**

Enables the user to control how exported CSV data appears in Notepad. Valid values are LF for a line feed between records and CRLF for a carriage return followed by a line feed.

- **Type:** string
- **Default value:** LF
- **Location:** System Property [sys_properties] table

**glide.csv.use_row_currency**

If false, exports currency and price field values in the user's currency. If true, exports currency and price field values in the currency of the row.

- **Type:** true | false
- **Default value:** false
- **Location:** System Property [sys_properties] table

**glide.custom.ip.authenticate.allow**

Comma-separated list or dash-separated range of IP addresses that are allowed access to view the stats.do, threads.do, and replication.do pages.

- **Type:** string
- **Default value:** none
- **Location:** Add the property **to the System Property [sys_properties] table.**
- **Instance Security Hardening Settings:** Performance monitoring IP restriction (instance security hardening)

**glide.db.aggregates.trend.use_iso_week**

If set to true, reports weekly trend by data according to ISO weeks. If false, data trended per week reports according to the first day of the week set by glide.ui.date_format.first_day_of_week.

- **Type:** true | false
- **Default value:** none
- **Location:** Add the property **to the System Property [sys_properties] table.**

**glide.db.audit.ignore.delete**

Specifies the tables where the sys_audit_delete file is not updated when records are deleted.

- **Type:** string — comma-separated list of tables
- **Location:** System Property [sys_properties] table

**glide.db.clone.allow_clone_target**

Enables (**true**) or disables (**false**) use of a non-production instance as the target for a system clone.

- **Type:** true | false
- **Default value:** **false** for production instances, **true** for non-production instances
**glide.db.impex.XMLLoader.max.file.size.mb**

Controls the maximum file size allowed when importing an XML file, in megabytes. Attempting to import an XML file larger than this limit results in an error.

- **Warning:** Use caution when modifying this property. Uploading a large XML file may impact performance and can cause an instance outage.
- Type: integer
- Default value: 100
- Location: System Properties > Import Export

**glide.db.large.threshold**

Sets the number of rows above which a table is considered large and uses a different method of querying for results. When this property is absent, the instance uses the default query method.

- Type: integer
- Default value: none
- Location: Add the property to the System Property [sys_properties] table.

**glide.db.loguser**

Display (true) or suppress display (false) of database errors (such as Unique Key violation detected by database (Duplicate entry 'ABC' for key 'name') to user.) to logged-in user.

- Type: true | false
- Default value: none
- Location: Add the property to the System Property [sys_properties] table.

**glide.db.max.aggregate.size**

Sets the maximum number of groups that a grouped report or list renders. Larger values may affect system performance.

- Type: integer
- Default value: 100
- Location: Add the property to the System Property [sys_properties] table.

**glide.db.max_view_records**

Sets the maximum number of records returned when running a GlideRecord query in a script. Do not use values larger than the default because they may cause queries to consume excessive memory on the application server and can, in extreme cases, cause a system outage. This property does not control the maximum number of records that appear in a list, report, or exported file.

- Type: integer
- Default value: 10000
- Location: Add the property to the System Property [sys_properties] table.

**glide.db.table.update_inactive_choices_enabled**

Specifies whether choice table selections marked as inactive (sys_choice inactive attribute = true) should be loaded into client databases when applications are installed (true) or not (false).
• Type: true | false
• Default value: true
• Location: System Property [sys_properties] table

**glide.debug.log_point**
Specifies whether the log points feature should be enabled or not.
• Type: true | false
• Default value: false
• Location: System Property [sys_properties] table

**glide.debugger.log.ui**
Specifies whether logs should be displayed under forms and lists and in the Session Log tab, or only in the Session Log tab.
• Type: choice list
• Default value: Page
• Location: System Property [sys_properties] table

**glide.discovery.application_mapping**
Enables or disables the Application Dependency Mapping (ADM) feature.
• Type: true | false
• Default value: true
• Location: System Property [sys_properties] table

**glide.discovery.log_debug_info**
An optional property to populate debug information in Discovery log. If this property is set to true, the Discovery sensor extracts the debug information from ECC input message and writes this information to the Discovery log table, so that it is visible when inspecting discovery status.
• Type: true | false
• Default: false

**glide.discovery.log_message_chars**
When a log message is longer than this value, ServiceNow creates a preview of the message with an ellipsis at the end of the message to indicate that there is content that is not shown. The preview size prevents any one list row from taking up the entire screen.
• Type: integer
• Default value: 200 (characters)
• Location: Discovery Definition > Properties

**glide.discovery.multi_page_serial_mode**
This property controls the processing of multi-page pattern input records. false sets the pages to process in parallel and true sets the pages to process serially.
• Type: true | false
• Default value: false

**glide.discovery.sam_batch_update_size**
Enables batching the updates to table cmdb_sam_sw_install when only the field last_scanned in the table has changed. This optimizes the overall discovery execution as it reduces the multiple single update queries on the database. The default value is 100 which means 100 records at a time in the table are batched and updated. By setting this property to 1, this switches to sequential updates.

- Type: integer
- Default value: 100

**glide.discovery.use_cmdb_identifiers**

Controls whether Discovery uses the CMDB Identification and Reconciliation Framework (introduced with the Geneva release) or the legacy identifiers from previous releases.

- Type: true | false
- Default value: true
- Location: **Discovery Definition > Properties**

**glide.domain.notify_change**

Displays a notification message telling the user that the domain picker automatically changed.

- Type: true | false
- Default value: true
- Location: Add the property to the System Property [sys_properties] table.

**glide.domain.notify_record_change**

Displays a notification message telling the user that the domain picker automatically changed because the record that the user is viewing changed the domain of the user.

- Type: true | false
- Default value: false
- Location: Add the property to the System Property [sys_properties] table.

**glide.duplicate_ci_remediator.dry_run**

Determines whether the Duplicate CI Remediator actually remediates CI duplication by updating records in the CMDB, or not.

- Type: true | false
- Default value: false
- Location: **Configuration > CMDB Properties > Duplicate CI Remediator Properties**

**glide.duplicate_ci_remediator.max.cis**

Threshold for the number of duplicate CIs, which if exceeded, support for reconciliation in the Duplicate CI Remediator is limited (1,000 by default).

- Type: integer
- Default value: 1000
- Location: **Configuration > CMDB Properties > Duplicate CI Remediator Properties**

**Note:** This threshold never exceeds 5,000, even if you set the property to a value greater than 5,000.

**glide.duplicate_ci_remediator.max.field_length**
Attributes in which max_length exceeds this property value (4000 by default) are excluded from the Select Master CI, Merge Attribute Values, and Determine Duplicate CI Actions tabs in the Duplicate CI Remediator wizard.

- Type: integer
- Default value: 4000
- Location: Configuration > CMDB Properties > Duplicate CI Remediator Properties

**Note:** This property impacts the performance of de-duplication tasks, therefore be cautious about setting this value.

`glide.duplicate_ci_remediator.related_items_blacklist`
Comma-separated list of related tables in the format `<table>,<reference column>`, that are excluded from merging during duplicate CI remediation.

- Type: string
- Default value: `cert_task.cmdb_ci,cert_audit_result.configuration_item,discovery_log.cmdb_ci,alm_hardware.ci,alm_asset.ci,fm_expense_line.ci`
- Location: Configuration > CMDB Properties > Duplicate CI Remediator Properties

`glide.eccprobe.longrunner.class`
Identifies the name of a script include that manages long running commands.

- Type: string
- Default value: LongRunner
- Location: System Property [sys_properties] table

`glide.eccprobe.longrunner.retry_minutes`
Allows bursts of polling errors up to specified minutes in duration.

- Type: integer
- Default value: 10
- Location: System Property [sys_properties] table

`glide.eccprobe.longrunner.interval.initial_seconds`
Initial polling period for long running commands in seconds.

- Type: integer
- Default value: 20
- Location: System Property [sys_properties] table

`glide.eccprobe.longrunner.interval.backoff_percent`
Percentage that polling period grows per poll.

- Type: integer
- Default value: 15
- Location: System Property [sys_properties] table

`glide.eccprobe.longrunner.interval.max_seconds`
Maximum polling period. As the polling period decays, it gets longer until it reaches this maximum.
• Type: integer
• Default value: 300
• Location: System Property [sys_properties] table

glide.eccprobe.longrunner.debug
Allows LongRunner logs status on successful polls in addition to the usual messages on unsuccessful ones when set to true.
• Type: true | false
• Default value: false
• Location: System Property [sys_properties] table

glide.eccprobe.longrunner.max_poll_count
Maximum number of polls that is executed per 5-second polling period. This number is generally not relevant, but may be used to contain polling under extreme loading conditions.
• Type: integer
• Default value: unlimited
• Location: System Property [sys_properties] table

glide.ecmdb.all_relationship_role
An example value is: itil,asset,configuration.
• Type: string
• Default value: none
• Location: Add the property to the System Property [sys_properties] table.

glide.email_address_filter.max_domains
Sets the maximum number of domains that can be associated with a single email address filter.
• Type: integer
• Default value: 100

glide.email_address_filter.max_exceptions
Sets the maximum number of exceptions that can be associated with a single email address filter.
• Type: integer
• Default value: 1000

glide.email.append.timezone
Specifies whether to append the time zone to all dates and times in outbound emails (true) or not (false).
• Type: true | false
• Default value: true
• Location: System Properties > Email

glide.email_client.quick_message.insert
Controls how quick messages are inserted in the email client. If the property is set to true, quick message content is inserted at the place of the cursor. If false, quick message content replaces existing content in an email draft.
• Type: true | false
• Default value: true

**glide.email.forward_subject_prefix**

Specifies the comma-separated list of prefixes in the subject line that identify a forwarded email.

- Type: string
- Default value: fw:,fwd:
- Location: Add the property to the System Property [sys_properties] table.

**glide.email.journal.lines**

Specifies the number of entries from a journal field (such as Additional comments and Work notes) included in email notifications. A value of -1 includes all journal entries.

- Type: integer
- Default value: 3
- Location: System Properties > Email

**glide.email.mail_to**

Specifies the email address to send notifications that use the `$mailto:` variable.

- Type: string
- Default value: SMTP email address that is active by default
- Location: Add the property to the System Property [sys_properties] table.

**glide.email.name_split**

Delimiter between the first and last name in an email address to identify users from incoming emails. For example, a delimiter of "." in the email address john.smith@company.com tells the system to look for a user record for John Smith.

- Type: string
- Default value: period (.)
- Location: System Properties > Email

**glide.email.notification.save_when_no_recipients**

Controls whether (true) or not (false) a notification-generated sys_mail record is saved even if there are no recipients. Used in conjunction with other notification recipient logging properties, this property enables troubleshooting problems with notifications.

- Type: true | false
- Default value: false
- Location: Add the property to the System Property [sys_properties] table.

**glide.email.override.url**

Sets the URL to use in emailed links in place of the instance URL. The URL should end with nav_to.do. An example value is: https://servicenow.customerdomain.com/production/nav_to.do.

- Type: string
- Default value: Instance URL
- Location: Add the property to the System Property [sys_properties] table.

**glide.email.read.active**
Enables (true) or disables (false) the inbound mail server.

- Type: true | false
- Default value: true
- Location: System Properties > Email

**glide.email.reply_subject_prefix**

Specifies the comma-separated list of prefixes in the subject line that identify an email reply.

- Type: string
- Default value: re:aw:,r:
- Location: System Property [sys_properties] table

**glide.email.smtp.active**

Specifies whether to enable (true) or disable (false) the outgoing mail server.

- Type: true | false
- Default value: true
- Location: System Properties > Email

**glide.email.smtp.max_recipients**

Specifies the maximum number of recipients the instance can list in the To: line for a single email notification. Notifications that would exceed this limit instead create duplicate email notifications addressed to a subset of the recipient list. Each email notification has the same maximum number of recipients.

- Type: integer
- Default value: 100
- Location: Add the property to the System Property [sys_properties] table.

**glide.email.smtp.max_send**

Specifies how many emails to send through each new SMTP connection. The instance establishes a new SMTP connection if there are more emails to send than the specified value.

- Type: integer
- Default value: 100
- Location: Add the property to the System Property [sys_properties] table.

**glide.email_system_address_filter.max_address_filters**

Sets the maximum number of email filters that can be associated with a single system address filter.

- Type: integer
- Default value: 100

**glide.email.test.user**

Specifies the comma-separated list of email addresses to which the instance sends all email messages. Typically used in non-production instances for testing purposes.

- Type: string
- Default value: none
- Location: System Properties > Email
glide.email.text_plain.strip_xhtml
Indicates whether both outbound and inbound emails that are shown in comments convert the XML to plain text (true) or preserve the XML (false).

- Type: true | false
- Default value: true
- Location: Add the property to the System Property [sys_properties] table.

Note: Glide emails are converted to plain text by default. Email clients that use the plain text version of the email show the watermark. Email clients that use the HTML version of an email do not display the watermark.

• Type: true | false
• Default value: false
• Location: System Property [sys_properties] table

glide.email.watermark.visible
Indicates whether the watermark in email notifications is visible (true) or is wrapped in a hidden div tag (false).

Note: Glide emails are converted to plain text by default. Email clients that use the plain text version of the email show the watermark. Email clients that use the HTML version of an email do not display the watermark.

• Type: true | false
• Default value: false
• Location: System Property [sys_properties] table

glide.email_client.show_sms_option
Specifies whether a check box appears in the email client for sending the message to the user's SMS device (true) or not (false). If no SMS device exists, the email client sends the message to the primary email device.

• Type: true | false
• Default value: false
• Location: System Property [sys_properties] table

glide.entry.loggedin.page_ess
Specifies the page that an ESS user, who by definition has no roles, is redirected to when the user logs in.

• Type: string
• Default value: none
• Location: System Property [sys_properties] table

glide.excel.boolean.display_value
If true, translates columns of type boolean to the user's language when exporting records in Excel format. If false, exports the values in English, regardless of the user language.

• Type: true | false
• Default value: false
• Location: System Property [sys_properties] table

glide.excel.max_cells
Sets the maximum number of cells in an Excel export.

• Type: integer
• Default value: 500000
• Location: Add the property to the System Property [sys_properties] table.

glide.excel.use_user_date_format
Specifies whether Excel exports use the date/time format specified in a user's profile (true) or not (false). If false, exports the instance date/time format defined by the glide.sys.date_format property.
• Type: true | false
• Default value: false
• Location: Add the property to the System Property [sys_properties] table.

**glide.export.csv.charset**

Specifies the character set used to export CSV files. See Supported Character Encodings for a list of supported character encoding options.

• Type: string
• Default value: windows-1252
• Location: Add the property to the System Property [sys_properties] table.

**glide.export.csv.raw.value**

When true, raw database values are exported instead of the display values when you export to CSV. When false, display values are exported.

• Type: true | false
• Default value: false
• Location: System Properties > Import Export

**glide.export.escape_formulas**

When true, string values that start with the characters +, -, =, or @ are prepended with a single apostrophe when you export to CSV, XLS, or XLSX files.

• Type: true | false
• Default value: true for new instances starting with Istanbul
• Location: System Property [sys_properties] table for new instances starting with Istanbul. For upgraded instances, Add the property to the System Property [sys_properties] table.

**glide.export.excel.general_formatting**

When true, values in cells in exported Excel files have the general format. When false, the cells in exported Excel files have the text format.

• Type: true | false
• Default value: false
• Location: Add the property to the System Property [sys_properties] table.

**glide.export.excel.wrap_cells**

When true, values in cells in exported Excel files are wrapped automatically. When false, the width of exported Excel columns is resized to fit 256 characters and values are not wrapped.

• Type: true | false
• Default value: true
• Location: Add the property to the System Property [sys_properties] table.

**glide.export.force_ui_list_behavior**

When true, journal fields such as worknotes and comments are not included when you export records. When false, these fields are included.

• Type: true | false
• Default value: true
• Location: Add the property to the System Property [sys_properties] table.

**glide.fdih.retry.max_count**

Specifies the maximum number of retry attempts when no value is specified in Count for a retry policy.

- Type: Integer
- Default value: 0
- Location: System Property [sys_properties] table

**glide.glidesoap.proxy_host**

Specifies the proxy server hostname or IP address for SOAP clients.

- Type: string
- Default value: value of glide.http.proxy_host
- Location: System Property [sys_properties] table

**glide.glidesoap.proxy_port**

Specifies the port number for the proxy server for SOAP clients.

- Type: string
- Default value: value of glide.http.proxy_port
- Location: System Property [sys_properties] table

**glide.guest.session_timeout**

Sets the session timeout for a guest session, in minutes.

**Note:** This setting decouples a guest session timeout from the glide.ui.session_timeout property. Any changes to the glide.ui.session_timeout property do not affect a guest session timeout.

- Type: integer
- Default value: 30
- Location: System Property [sys_properties] table

**glide.help.default.page**

Sets the overall help URL for the system if you are using context-sensitive help. This URL is used when there is not any context-sensitive help available for the form, list, or record.

- Type: string
- Default value: http://wiki.servicenow.com/
- Location: System Property [sys_properties] table

**glide.history.max_entries**

Sets the number of characters to display as a preview of journal input fields.

- Type: integer
- Default value: 250
- Location: System Property [sys_properties] table

**glide.home.page**

Specifies which page to load when a user selects a homepage from the banner.
• Type: string
• Default value: `home_splash.do?sysparm_direct=true`
• Location: System Property [sys_properties] table

**glide.home.refresh_disabled**
Enables (true) or disables (false) homepage refresh.

• Type: true | false
• Default value: false
• Location: System Property [sys_properties] table

**glide.home.refresh_intervals**
Comma-separated list of refresh intervals available on homepages.

• Type: string
• Default value: 300,900,1800,3600
• Location: Add the property to the System Property [sys_properties] table.

**glide.html.enable_media_sites**
Enables a URL option for media in the HTML Editor. The media attaches, but doesn't load in the HTML Editor.

• Type: string
• Default value: `youtube.com,player.vimeo.com,vimeo.com`
• Location: System Property [sys_properties] table

**glide.html.escape_script**
Enables (true) or disables (false) JavaScript tags in HTML fields.

• Type: true | false
• Default value: true
• Location: System Property [sys_properties] table

**glide.html.sanitize_all_fields**
Specifies whether all HTML fields are sanitized to remove unwanted code (true) or not (false).

• Type: true | false
• Default value: true
• Location: System Property [sys_properties] table

- Instance Security Hardening Settings: HTML sanitizer (instance security hardening)

**glide.http.connection_timeout**
Specifies the maximum number of milliseconds an outbound HTTP request (such as Web Services) waits to establish a connection.

• Type: integer
• Default value: 10000 (10 seconds)
• Location: System Property [sys_properties] table

**glide.http.outbound.max_timeout**
Specifies the number of seconds that RESTMessageV2 and SOAPMessageV2 APIs wait for a response from a synchronous call. The maximum value is 30 seconds.
To define a timeout longer than 30 seconds, set the `glide.http.outbound.max_timeout.enabled` system property to `false` and use the `waitForResponse()` method to set the timeout. For examples, see [Asynchronous RESTMessageV2 example](#) and [Asynchronous SOAPMessageV2 example](#). If `glide.http.outbound.max_timeout.enabled` is set to `true` and a value is passed in the `waitForResponse()` method, the system uses the smallest value from either the `waitForResponse()` method or the `glide.http.outbound.max_timeout` system property.

- **Type:** `integer`
- **Default value:** 30
- **Location:** Add the property to the System Property `[sys_properties]` table.

### `glide.http.outbound.max_timeout.enabled`

Enables setting a timeout in the `glide.http.outbound.max_timeout` system property.

To define a timeout longer than 30 seconds, set the `glide.http.outbound.max_timeout.enabled` system property to `false` and use the `waitForResponse()` method to set the timeout. For examples, see [Asynchronous RESTMessageV2 example](#) and [Asynchronous SOAPMessageV2 example](#). If `glide.http.outbound.max_timeout.enabled` is set to `true` and a value is passed in the `waitForResponse()` method, the system uses the smallest value from either the `waitForResponse()` method or the `glide.http.outbound.max_timeout` system property.

- **Type:** `boolean`
- **Default value:** `true`
- **Location:** Add the property to the System Property `[sys_properties]` table.

### `glide.http.proxy_bypass_list`

Specifies the semicolon-separated list of addresses that bypass the proxy server. Use an asterisk (*) as a wildcard character to specify all or part of an address.

- **Type:** `string`
- **Default value:** `none`
- **Location:** System Property `[sys_properties]` table

### `glide.http.proxy_host`

Specifies the proxy server hostname or IP address.

- **Type:** `string`
- **Default value:** `none`
- **Location:** System Property `[sys_properties]` table

### `glide.http.proxy_ntdomain`

Specifies the domain used to authenticate the proxy server with NTLM authentication.

- **Type:** `string`
- **Default value:** `none`
- **Location:** System Property `[sys_properties]` table

### `glide.http.proxy_nthost`

Specifies the hostname used to authenticate the proxy server with NTLM authentication.

- **Type:** `string`
- **Default value:** `none`
• Location: System Property [sys_properties] table

**glide.http.proxy_ntpassword**

Specifies the password used to authenticate the proxy server with NTLM authentication.

- Type: string
- Default value: none
- Location: System Property [sys_properties] table

**glide.http.proxy_ntusername**

Specifies the user name used to authenticate the proxy server with NTLM authentication.

- Type: string
- Default value: none
- Location: System Property [sys_properties] table

**glide.http.proxy_port**

Specifies the port number for the proxy server.

- Type: string
- Default value: none
- Location: System Property [sys_properties] table

**glide.http.proxy_password**

Specifies the password used to authenticate the proxy server.

- Type: string
- Default value: none
- Location: System Property [sys_properties] table

**glide.http.proxy_username**

Specifies the username used to authenticate the proxy server.

- Type: string
- Default value: none
- Location: System Property [sys_properties] table

**glide.http.timeout**

(Web service Consumer Plugin) Specifies the maximum number of milliseconds to wait before an outbound transaction times out.

- Type: integer
- Default value: 175000 (175 seconds)
- Location: Add the property to the System Property [sys_properties] table.

**glide.i18n.force_index**

Enables (true) or disables (false) indexing all translated fields, regardless of the value of the table attribute text_index_translations.

- Type: true | false
- Default value: true
**glide.identification_engine.batch_update_last_discovered**

Controls batch update of last_discovered field in CIs that are being processed by the identification engine.

Set to **false** if there are business rules that apply to last_discovered field, and you want to trigger these rules when calling Identification and Reconciliation API.

- Type: true | false
- Default value: true
- Location: Add the property to the System Property [sys_properties] table.

**glide.identification_engine.dependent_items_local_cache_count**

For optimization, a custom number of locally cached query result entries of dependent CIs.

- Type: integer
- Default value: 10000
- Location: Add the property to the System Property [sys_properties] table.

**Note:** If there is a memory issue due to optimization related to using local cache, set the **glide.identification_engine.related_items_local_cache_count** and the **glide.identification_engine.dependent_items_local_cache_count** properties to 0.

**glide.identification_engine.granular_insert_locking**

Determines whether to use multiple granular insert locks or single global insert lock.

Set to **false** if there are performance issues associated with the usage of multiple granular insert locks.

- Type: true | false
- Default value: true
- Location: Add the property to the System Property [sys_properties] table.

**glide.identification_engine.independent_items_local_cache_count**

For optimization, a custom number of locally cached query result entries of independent CIs.

- Type: integer
- Default value: 100000
- Location: Add the property to the System Property [sys_properties] table.

**Note:** Setting the value to 0 avoids using local cache for independent CIs and might affect performance.

**glide.identification_engine.related_items_local_cache_count**

For optimization, a custom number of locally cached query result entries of related/lookup items.

- Type: integer
- Default value: 15000
- Location: Add the property to the System Property [sys_properties] table.

**Note:** If there is a memory issue due to optimization related to using local cache, set the **glide.identification_engine.related_items_local_cache_count** and the **glide.identification_engine.dependent_items_local_cache_count** properties to 0.
**glide.identification_engine.skip_duplicates**

Controls how identification processes a small set of duplicate CIs.

- **When true:** If the number of duplicate CIs is less than the threshold specified by `glide.identification_engine.skip_duplicates.threshold`, then one of the duplicate CIs is picked as a match and gets updated. The rest of the duplicate CIs are tagged as duplicates.
- **When false:** Matching a CI fails, and an error is logged.

- Type: true | false
- Default value: true
- Location: Add the property to the System Property [sys_properties] table.

**glide.identification_engine.skip_duplicates.threshold**

Maximum number of CIs that can be in a set of duplicate CIs to allow identification to process the duplicate CIs according to the setting of `glide.identification_engine.skip_duplicates`. If the number of duplicate CIs exceeds the threshold, then identification processes the duplicate CIs as if `glide.identification_engine.skip_duplicates` is set to false, regardless of the setting.

- Type: integer
- Default value: 5
- Location: Add the property to the System Property [sys_properties] table.

**glide.identification_logs.max_run_ids**

Maximum number of log runs that can be displayed when navigating to Configuration > Identification Logs.

- Type: integer
- Default value: 1000
- Location: Configuration > CMDB Properties > Identification/Reconciliation Properties.

**glide.image_provider.security_enabled**

Controls the security settings for images. If true, images are visible only to authenticated and authorized users. If false, images are visible to anyone with a URL to the attachment.

- Type: true | false
- Default value: true
- New/zbooted instances: property is present and set to true
- Upgraded instances: false if property is not present, unchanged if property is present
- Location: System Property [sys_properties] table

**glide.imap.secure**

Enables (true) or disables (false) SSL encryption for connections to the IMAP server.

- Type: true | false
- Default value: false
- Location: Add the property to the System Property [sys_properties] table.

**glide.imap.secure_port**

 Specifies the communications port for IMAP secure connections.

- Type: string
• Default value: 995
• Location: Add the property to the System Property [sys_properties] table.

**glide.imap.tls**
Enables (true) or disables (false) starting the IMAP server in Transport Layer Security (TLS) mode.
• Type: true | false
• Default value: false
• Location: Add the property to the System Property [sys_properties] table.

**glide.import.debug**
Enables (true) or disables (false) debug logging for all import processes.
• Type: true | false
• Default value: false
• Location: Add the property to the System Property [sys_properties] table.

**glide.import.error_message.generic**
Enables (true) or disables display (false), failed imports to display a generic error instead of a verbose SQL message. This property should be enabled.
• Type: true | false
• Default value:
  • New/zbooted instances: true for starting with Istanbul
  • Upgraded instances: false
• Location: System Property [sys_properties] table

**glide.import.excel.use_only_user_session_date_format**
If true, any Date or Date/Time value in an Excel spreadsheet is converted to a user session date format in the staging table upon Excel file import.
If false, any Date/Time explicit cell type in Excel is imported into a staging table with the user session date format, and any date value that is not explicitly in a Date/Time cell type in Excel is imported into a staging table using the system date format.
• Type: true | false
• Default value: true
• Location: Add the property to the System Property [sys_properties] table if you want to change the value to false.

**glide.import.sftp.debug**
Enables (true) or disables (false) additional debug logging for SFTP imports. Enabling this property causes the instance to log all outgoing and incoming messages during the SSH session.
• Type: true | false
• Default value: false
• Location: Add the property to the System Property [sys_properties] table.

**glide.importscp.debug**
Enables (true) or disables (false) additional debug logging for SCP imports. Enabling this property causes the instance to log all outgoing and incoming messages during the SSH session.
• Type: true | false
• Default value: false
• Location: Add the property to the System Property [sys_properties] table.

**glide.import_set.preserve.leading.spaces**

Specifies whether the import process preserves leading spaces in Excel data cells (true) or not (false). When false, the import process removes leading spaces from Excel data cells.

Note: The import process always removes trailing spaces from Excel data cells.

• Type: true | false
• Default value: false
• Location: Add the property to the System Property [sys_properties] table.

**glide.import_set_row.dynamically_add_fields**

Specifies whether an import set can add new columns to the staging table (true) or not (false). Instances that contain large numbers of import sets can sometimes become unresponsive when an import adds a column because the instance must alter every row in the staging table. Sometimes the database alter table action causes an outage. Setting this property to false prevents an import set from adding columns to the staging table and produces a log message. As a workaround, administrators can manually add a column to the staging table by creating a new dictionary entry and then reimporting the import set.

• Type: true | false
• Default value: false
• Location: Add the property to the System Property [sys_properties] table.

**glide.ir.query_method**

Sets the query method for global text search. Only the Simple query method is supported.

• Type: choice list
• Default value: simple
• Location: System Properties > Global Text Search

**glide.integration.session_timeout**

Length of time, in minutes, that an inactive integration session is maintained before the session times out.

• Type: integer
• Default value: 1
• Location: Add the property to the System Property [sys_properties] table.

**glide.invalid_query.returns_no_rows**

Controls how invalid GlideRecord queries are handled with respect to invalid or undefined field names. When this property is true, invalid queries containing invalid or undefined field names always return no rows. When this property is false (default), if a query is incorrect, and includes invalid or undefined field names, the invalid part of the query condition is ignored and results are based on the valid part of the query.

To override this logic at the session level, execute `gs.getSession().setStrictQuery(false)`. To restore strict query, execute `gs.getSession().setStrictQuery(true)`. To use this property, change the line `gr.addQuery('table', arguments.length == 1 ? record.getRecordClassName() :`
gr.addQuery('table', (tableName) ? tableName : record.getRecordClassName() );

- Type: true | false
- Default value: false
- Location: Add the property to the System Property [sys_properties] table.

glide.itil.assign.number.on.insert

Controls whether (true) or not (false) a task number is generated and assigned on load (Create New) or when the task is submitted. This feature helps prevent unused task numbers.

- Type: true | false
- Default value: false
- Location: System Property [sys_properties] table

glide.jdbcprobeloader.retry

Sets the number of times a JDBC probe attempts to connect to a JDBC data source.

- Type: integer
- Default value: 60
- Location: Add the property to the System Property [sys_properties] table.

glide.jdbcprobeloader.retry_millis

Sets the number of milliseconds a JDBC probe waits between retry attempts to a JDBC data source.

- Type: integer
- Default value: 5000
- Location: Add the property to the System Property [sys_properties] table.

glide.jquery.legacy

When true, enables legacy Jquery behavior. When false, integrates the Jquery 1.12.3 and 2.2.3 security patches. If you set this property to false, UI pages with incorrect HTML markup may render incorrectly. You can address this issue in your scripts by closing any html element tags that are self-closing and not in the valid list. For example, change <div /> to <div></div>. Valid self-closing elements that do not need to be updated include:

- <area />
- <base />
- <br />
- <col />
- <embed />
- <hr />
- <img />
- <input />
- <link />
- <meta />
- <param />
- <source />
- <track />
- <wbr />

- Type: true | false
- Default value: true
• Location: System Property [sys_properties] table

**glide.knowman.search.apply_role_based_security**

If **true**, honors read access of knowledge bases or articles specified for roles. If **false**, enables specified user criteria to override read access specified for roles.

- Type: true | false
- Default value: true
- Location: Add the property to the System Property [sys_properties] table.

**glide.knowman.search.character_limit**

Minimum number of characters required for knowledge search. Search terms with fewer than this number of characters return no results.

- Type: integer
- Default value: 3
- Location: System Property [sys_properties] table

**glide.knowman.search.default_language**

(Knowledge Management Internationalization Plugin v2) Default language for knowledge articles. If empty, defaults to the language of the logged-in user.

- Type: string
- Default value: empty
- Location: System Property [sys_properties] table

**glide.knowman.show_language_option**

(Knowledge Management Internationalization Plugin v2) Specifies whether the **Language** box appears (true) or is hidden (false) on articles with multiple translations.

- Type: true | false
- Default value: false
- Location: Add the property to the System Property [sys_properties] table.

**glide.knowman.show_language_option.roles**

(Knowledge Management Internationalization Plugin v2) Comma-separated list of roles that can see the Language box on articles with multiple translations.

- Type: string
- Default value: none
- Location: Add the property to the System Property [sys_properties] table.

**glide.knowman.show_links**

Specifies whether the **Link** line appears (true) or is hidden (false) in a knowledge article.

- Type: true | false
- Default value: true
- Location: System Property [sys_properties] table

**glide.ldap.allow_empty_group**

Specifies whether all members can be removed from an Active Directory security group (true) or not (false).
• Type: true | false
• Default value: true
• Location: Add the property to the System Property [sys_properties] table.

**glide.ldap.binary_attributes**

Comma-separated list of LDAP attributes that should be converted from binary format to encoded64 strings. If you set this property, only the values listed are converted. The most common attributes are objectSID and objectGUID. These converted values are unique and can be used as the coalesce field on the LDAP import mapping. If this property is blank, ServiceNow tries to map these binary attributes without the conversion and they are not guaranteed to be unique since they are not properly converted to string values.

• Type: string
• Default value: objectsid,objectguid
• Location: System Property [sys_properties] table

**glide.ldap.paging**

 Enables (true) or disables (false) LDAP paging query support. LDAP paging is a more efficient LDAP querying method for environments with more than 1000 users.

• Type: true | false
• Default value: true
• Location: System Property [sys_properties] table

**glide.legacy.excel.export**

 Enables (true) or disables (false) exporting to XLS format when exporting to an Excel file. By default, only XLSX export is enabled. This property does not affect the Excel web service. When true, this property also allows users to select XLS or XLSX as the Easy Import template format.

• Type: true | false
• Default value: false
• Location: Add the property to the System Property [sys_properties] table.

**glide.list.filter_max_length**

Sets a maximum character limit for the condition builder query.

• Type: integer
• Default value: 0
• Location: System Property [sys_properties] table

**glide.lists.live_list_enabled**

Enables a list refresh prompt.

• Type: true | false
• Default value: false
• Location: System Property [sys_properties] table

**glide.live_feed.company_feed_exclude_groups**

Controls whether messages posted to a public group appear (true) or are omitted (false) on the Company Feed.

• Type: true | false
• Default value: true
• Location: System Property [sys_properties] table

glide.live_services
(Chat plugin) Enables (true) or disables (false) Live Services, such as chat support.
• Type: true | false
• Default value: false
• Location: Add the property to the System Property [sys_properties] table.

glide.login.no_blank_password
Prevents (true) or allows (false) logins from users with blank passwords. Often, importing lists of users creates many users with blank passwords. By default, this property is set to true on production instances.
• Type: true | false
• Default value: true
• Location: System Property [sys_properties] table

glide.login.home
Sets the default homepage that users see after login. If blank, the last page visited is used. The format is <page>.do.
• Type: string
• Default value: home.do
• Location: System Property [sys_properties] table

glide.max_journal_list_size
Sets the maximum size, in megabytes, of journal input fields.
• Type: integer
• Default value: 10
• Location: Add the property to the System Property [sys_properties] table.

glide.messaging.reassign.enabled
Sets property that automatically reassigns messaging if the current agent is unavailable.
• Type: true | false
• Default value: false
• Location: System Property [sys_properties] table

glide.notification.recipient.include_logging
Master switch to enable/disable logging all reasons a recipient was included. If false, no include logging is performed.
• Type: true | false
• Default value: true
• Location: Add the property to the System Property [sys_properties] table.

glide.notification.recipient.exclude_logging
Master switch to enable/disable logging all reasons a recipient was excluded. If false, no exclude logging is performed.
• Type: true | false
• Default value: true
• Location: Add the property to the System Property [sys_properties] table.

**glide.notification.recipient.exclude_logging.device_inactive**
Logs recipients who are excluded because their chosen notification device record is marked as inactive.

• Type: true | false
• Default value: true

The glide.notification.recipient.exclude_logging property in the System Properties > Email module must be enabled to modify this property.

**glide.notification.recipient.exclude_logging.device_schedule**
Logs recipients who are excluded because the chosen notification device record’s schedule field excludes it.

• Type: true | false
• Default value: true

The glide.notification.recipient.exclude_logging property in the System Properties > Email module must be enabled to modify this property.

**glide.notification.recipient.exclude_logging.event_creator**
Logs recipients who are excluded because they initiated the notification event, such as updating an incident record, and the Send to Event Creator check box is cleared on the notification record.

• Type: true | false
• Default value: true

The glide.notification.recipient.exclude_logging property in the System Properties > Email module must be enabled to modify this property.

**glide.notification.recipient.exclude_logging.invalid_email**
Logs recipients who are excluded because the email address for that user is invalid, for example the @ is missing, or empty.

To modify this property, you must enable the glide.notification.recipient.exclude_logging property in the System Properties > Email module.

• Type: true | false
• Default value: true

**glide.notification.recipient.exclude_logging.user_calendar_integration_disabled**
Logs recipients of calendar invitations who are excluded because the Calendar Integration field is set to None on the user record.

• Type: true | false
• Default value: true

The glide.notification.recipient.exclude_logging property in the System Properties > Email module must be enabled to modify this property.

**glide.notification.recipient.exclude_logging.user_inactive**
Logs recipients who are excluded because the Active check box is cleared on the user record.

• Type: true | false
• Default value: true

The `glide.notification.recipient.exclude_logging` property in the [System Properties > Email](#) module must be enabled to modify this property.

### glide.notification.recipient.exclude_logging

Logs recipients who are excluded because the [Notification](#) field is set to [Disabled](#) on the user record.

To modify this property, you must enable the `glide.notification.recipient.exclude_logging` property in the [System Properties > Email](#) module.

- **Type:** true | false
- **Default value:** true

### glide.notification.recipient.include_logging

Enables or disables logging all reasons that a recipient was included. This property is a master switch. If **true**, the subsequent properties dealing with the inclusion of logging are enabled. If **false**, none of the subsequent properties relating to the inclusion of logging are enabled.

### glide.notification.recipient.include_logging.delegate

Logs recipients who are included because they are delegates of another user.

- **Type:** true | false
- **Default value:** true

The `glide.notification.recipient.include_logging` property in the [System Properties > Email](#) module must be enabled to modify this property.

### glide.notification.recipient.include_logging.event_parm

Logs recipients who are included because they are in the `parm1` or `parm2` fields of the event record.

To modify this property, you must enable the `glide.notification.recipient.include_logging` property in the [System Properties > Email](#) module.

- **Type:** true | false
- **Default value:** true

### glide.notification.recipient.include_logging.recipient_fields

Logs recipients who are included via a notification target record, such as an incident record, specified in the [Users/Groups in Field](#) field for the notification record. The `recipient_fields` are fields in the target record that contain a recipient to add. For example, if the record that triggered the notification is an incident, and the `assigned_to` field for the incident is listed in `recipient_fields`, that user is included as a recipient.

To modify this property, you must enable the `glide.notification.recipient.include_logging` property in the [System Properties > Email](#) module.

- **Type:** true | false
- **Default value:** true

### glide.notification.recipient.include_logging.recipient_groups.group_email

Logs recipients who are included in a group email for any group provided in the notification record’s `recipient_groups` or the event `parm1` or `parm2` field.
To modify this property, you must enable the `glide.notification.recipient.include_logging` property in the **System Properties > Email** module.

- **Type:** true | false
- **Default value:** true

**glide.notification.recipient.include_logging.recipient_groups.manager**

Logs recipients who are included because they manage any group provided in the notification record’s `recipient_groups` or the event `parm1` or `parm2` field.

To modify this property, you must enable the `glide.notification.recipient.include_logging` property in the **System Properties > Email** module.

- **Type:** true | false
- **Default value:** true

**glide.notification.recipient.include_logging.recipient_groups.membership**

Logs recipients who are included via membership in any group provided in the notification record `recipient_groups` or the event `parm1` or `parm2` field.

To modify this property, you must enable the `glide.notification.recipient.include_logging` property in the **System Properties > Email** module.

- **Type:** true | false
- **Default value:** true

**glide.notification.recipient.include_logging.recipient_users**

Logs recipients who are included via notification record’s `Users` field (`recipient_users`).

To modify this property, you must enable the `glide.notification.recipient.include_logging` property in the **System Properties > Email** module.

- **Type:** true | false
- **Default value:** true

**glide.notification.recipient.include_logging.subscription**

Logs recipients because they are subscribed via User Notification Preferences.

To modify this property, you must enable the `glide.notification.recipient.include_logging` property in the **System Properties > Email** module.

- **Type:** true | false
- **Default value:** true

**glide.pdf_export_from_form_list.show_report_attrs**

Enables or disables displaying the PDF page header for all PDFs generated from a list.

- **Type:** true | false
- **Default value:** true
- **Location:** System Property [sys_properties] table

**glide.pdf.max_rows**

Sets the maximum number of rows in an exported PDF file.

- **Type:** integer
- Default value: 1000
- Location: Add the property to the System Property [sys_properties] table.

**glide.pdf.font.size**

Sets the font size for exported PDF files.
- Type: integer
- Default value: 8
- Location: Add the property to the System Property [sys_properties] table.

**glide.pg.any_rejection_rejects**

Controls the default process guide rejection handling. If `true`, the first rejection rejects the entity. If `false`, all users must reject the approval.
- Type: true | false
- Default value: true
- Location: System Property [sys_properties] table

**glide.phone_number_e164.allow_national_entry**

When `true`, users can enter phone numbers in the local format listed in the territory selector. When `false`, users must enter phone numbers in the international format listed in the territory selector.
- Type: true | false
- Default value: true
- Location: Add the property to the System Property [sys_properties] table.

**glide.phone_number_e164.display_national**

When set to `true` or `form`, a Phone Number (E164) field displays phone numbers in a local format on forms but as an international format on lists. When set to `all`, a Phone Number (E164) field always displays phone numbers in a local format. When set to user, a Phone Number (E164) field only displays phone numbers in a local format when the phone number matches the locale setting of the current user.
- Type: string
- Default value: false
- Location: Add the property to the System Property [sys_properties] table.

**glide.phone_number_e164.display_territory_selector**

Specifies whether to display (true) or hide (false) the territory selector. Hiding the territory selector restricts users to entering only local or national phone numbers.
- Type: true | false
- Default value: true
- Location: Add the property to the System Property [sys_properties] table.

**glide.phone_number_e164.display_territory_text**

When set to all, a Phone Number (E164) always displays the territory label. When set to national, a Phone Number (E164) displays the territory label only if the phone number is in local format. When set to read-only, a Phone Number (E164) displays the territory label in read-only mode regardless of whether the number is in local or global format. When set to read-only-national, a Phone Number (E164) displays the territory label in read-only mode only if the number is in local format. When set to list, a Phone Number (E164) displays the territory label in a list. When set to list-national, a Phone Number (E164) displays territory label in a list if the number is in national format. When set to none, a Phone Number (E164) does not display the territory label.
• Type: string
• Default value: read-only
• Location: Add the property to the System Property [sys_properties] table.

**glide.phone_number_e164.display_users_idd**

Specifies whether to display the international direct dialing prefix between the territory selector and the input box on forms (true) or not (false).

• Type: true | false
• Default value: false
• Location: Add the property to the System Property [sys_properties] table.

**glide.phone_number_e164.strict**

Specifies whether all phone number fields must match the display format of the field's select territory. When true, the phone number input box displays a red line underneath phone numbers that do not match the territory format listed in the territory selector. Users cannot save an invalid phone number. When false, the phone number input box displays a green line underneath phone numbers that do not match the territory format listed in the territory selector. Users can save an invalid phone number, and the territory selector offers the option to select an Other / Unknown territory format.

• Type: true | false
• Default value: true
• Location: Add the property to the System Property [sys_properties] table.

**glide.pop3.ignore_headers**

Specifies the comma-separated list of email headers that cause the instance to ignore an email message. Use the format name:value to specify email header types and values. You can use a wildcard (*) for the subtype. For example, Content-Type:multipart/*; report-type=delivery-status; ignores emails containing a type of multipart and a parameter of report-type=delivery-status. For syntax specifications, see http://www.w3.org/Protocols/rfc1341/4_Content-Type.html.

• Type: string
• Default value: Auto-Submitted:auto-replied,X-FC-MachineGenerated:true,Content-Type:multipart/report; report-type=delivery-status;
• Location: System Properties > Email

**glide.pop3.ignore_senders**

Specifies the comma-separated list of senders that cause the instance to ignore an email message. Enter only the name before the at (@) sign.

• Type: string
• Default value: mailer-daemon, postmaster
• Location: System Properties > Email

**glide.pop3.ignore_subjects**

Specifies the comma-separated list of strings that cause the instance to ignore an email message if they are present at the start of a subject line. Values are case-insensitive.

• Type: string
• Default value: out of office autoreply, undeliverable:, delivery failure:,returned mail:,autoreply
• Location: System Properties > Email
**glide.pop3.parse_end**

[Legacy] Text indicating the end of the email body section where the instance should parse name:value pairs to change field values when processing inbound email actions. This property is no longer required to set field values from the email body.

- Type: string
- Default value: none
- Location: System Properties > Email

**glide.pop3.parse_start**

[Legacy] Text indicating the beginning of the email body section where the instance should parse name:value pairs to change field values when processing inbound email actions. This property is no longer required to set field values from the email body.

- Type: string
- Default value: none
- Location: System Properties > Email

**glide.pop3.process_locked_out**

Enables (true) or disables (false) the ability for locked out users to trigger inbound actions.

- Type: true | false
- Default value: false
- Location: System Property [sys_properties] table

**glide.pop3.reply_separators**

Comma-separated list of separators that cause the instance to disregard everything below the text string in the message body. This list is case-sensitive.

- Type: string
- Default value: \n\n-----Original Message-----,\n\n_____ 

From:
- Location: System Properties > Email

**glide.pop3readerjob.create_caller**

Controls the behavior when an instance receives an email from an email address not associated with a user record. If true, the instance creates a new user record for the email address and places that new user in the Caller field of any created tickets. If false, the instance associates the new ticket to the Guest user record.

- Type: true | false
- Default value: false
- Location: System Properties > Email

**glide.processor.json.row_limit**

Specifies the maximum number of rows a JSON query returns.

- Type: integer
- Default value: 250
- Location: Add the property to the System Property [sys_properties] table.

**glide.product.description**

The value of this property is displayed as text in the banner next to the company logo.
- Type: string
- Default value: Service Management
- Location: System Properties > Basic Configuration UI16

**glide.product.help_url**

Global setting for the URL that the help icon goes to. Value must be empty for context-sensitive help to work.

**glide.product.help_show**

Controls whether the help icon, help.gifx, appears in (true) or is omitted from (false) the welcome banner.

- Type: true | false
- Default value: true
- Location: System Property [sys_properties] table

**glide.product.image.light**

The Banner image displayed for UI16 Interface.

- Type: uploaded image
- Default value: none
- Location: System Properties > Basic Configuration UI16

**glide.product.icon**

Stores the favicon image displayed in bookmarks, tabs, and the browser address bar.

- Type: image
- Default value: favicon.ico?v=4
- Location: System Properties > System

**glide.product.name**

Specifies text to use in place of Service-now.com in the browser top title bar (and in browser tabs). This text is duplicated in the banner to the right of the logo unless you add display: none; to the end of the value field within the glide.product.name.style property.

- Type: string
- Default value: ServiceNow
- Location: System Property [sys_properties] table

**glide.product.name.style**

Specifies the CSS properties used to display the glide.product.name text in the banner to the right of the logo. To not display the text, add display: none; to the end of the value field in this property.

- Type: string
• Default value: padding-bottom: 0px; padding-top: 0px;
• Location: System Property [sys_properties] table

glide.quota.manager.debug
Controls whether to display (true) or hide (false) additional information related to the Quota Manager, such as running transactions, canceled transactions, and which quotas are matched to transactions.
• Type: true | false
• Default value: true
• Location: Add the property to the System Property [sys_properties] table.

glide.quota.manager.heartbeat
Sets the number of seconds between the start of each Quota Manager heartbeat. This value determines how often the Quota Manager checks for transactions exceeding a quota and how often the Quota Manager writes status in the log file.
• Type: integer
• Default value: 1
• Location: Add the property to the System Property [sys_properties] table.

glide.quota.manager.minimum_transaction_time
Sets the minimum number of seconds that a transaction must run before the Quota Manager matches it to a transaction quota. You should set this value to at least 1 second because smaller values decrease performance, and because transactions shorter than 1 second are probably not worth canceling. For optimal performance, set this value to the value of your most restrictive quota. For example, if your most restrictive quota cancels transactions longer than 1 minute, set the minimum transaction time to 60 seconds.
• Type: integer
• Default value: 1
• Location: Add the property to the System Property [sys_properties] table.

glide.reconciliation.override.null
Flag for allowing or disallowing the update of an empty field by a lower priority data source.
• Type: true | false
• Default value: true
• Location: System Properties [sys_properties] table

glide.remote_glide_record.max_count
Control the maximum number of records that the GlideRecord query method returns when using the SOAP web service. The instance primarily uses this property to control the records returned when using a Perl API GlideRecord query.

⚠️ Warning: If you set this property to a large value, such as 10000, socket timeout errors might occur with MID Servers. Keep the value of this property less than 1000.
• Type: integer
• Default value: 250
• Location: Add the property to the System Property [sys_properties] table.

glide.report.add_to_list_supported
Sets whether to support the add_to_list ACL for reporting on specified columns from the Available columns list when creating or sharing a list report.

- Type: true | false
- Default value: false
- Location: System Property [sys_properties] table

**glide.report.calendar.max_more_events_per_day**

Specifies the maximum number of calendar events that can appear in the + <number> pop-up for:

- A calendar day when calendar is in month or year view
- The top 'full day' section of a calendar day when a calendar is in day or week view

When this number is exceeded, a + many link appears, which opens a list of events instead of a pop-up. For more information about the maximum number of events that can be displayed in a calendar day, see system property **glide.report.calendar.max_events_displayed_per_cell**.

- Type: integer
- Default value: 30
- Location: Add the property to the System Property [sys_properties] table.

**glide.report.calendar.max_events_displayed_per_cell**

Defines the maximum number of events that can appear in calendar report for:

- A calendar day when calendar is in month or year view
- The top 'full day' section of a calendar day when a calendar is in day or week view

Events that exceed this value are visible via a link in the calendar cell. See **glide.report.calendar.max_more_events_per_day** for more information.

- Type: integer
- Default value: 3
- Location: Add the property to the System Property [sys_properties] table.

**glide.report.new_calendar**

Enables (true) or disables (false) new calendar reports. Internet Explorer 7 and 8 do not support new calendars. If you open a calendar report in one of these browsers, the old version of calendar reports is always used.

- Type: true | false
- Default value: true
- Location: System Property [sys_properties] table

**glide.report_home.group_report.show_usr_grp**

Enables (true) or disables (false) the Reporting preferences link in the user profile.

- Type: true | false
- Default value: false
- Location: System Property [sys_properties] table

**glide.required.attribute.enabled**

Flag for enforcing required attributes (cannot be null) during identification and reconciliation.

- Type: true | false
• Default value: true
• Location: System Properties [sys_properties] table.

**glide.rest.apis.disabled**

Controls which REST APIs are available on the instance, along with glide.rest.apis.enabled. The value for this property is a comma-separated list of API names, such as Table API or Aggregate API. If neither this property nor glide.rest.apis.enabled is set, all REST APIs are available. If a particular API is specified in both properties, that API is disabled. If you disable specific APIs without explicitly enabling any APIs, all REST APIs except the disabled APIs are available.

• Type: string
• Default value: all REST APIs are enabled by default
• Location: System Property [sys_properties] table

**glide.rest.apis.enabled**

Controls which REST APIs are available on the instance, along with glide.rest.apis.enabled. The value for this property is a comma-separated list of API names, such as Table API or Aggregate API. If neither this property nor glide.rest.apis.disabled is set, all REST APIs are available. If a particular API is specified in both properties, that API is disabled. If you enable specific APIs, only those APIs are available.

• Type: string
• Default value: all REST APIs are enabled by default
• Location: Add the property to the System Property [sys_properties] table.

**glide.rest.choice.allow_non_existing_value**

Enables passing non-existing values to a choice field.

• Type: true | false
• Default value: false

  If true, the choice field is set to a passed value, even if the passed value does not exist in the choice field.
• Location: Add the property to the System Property [sys_properties] table.

**glide.rest.debug**

Logs all stages of REST processing, including processing times.

• Type: true | false
• Default value: false
• Location: Add the property to the System Property [sys_properties] table.

**glide.rollback.version**

Controls whether rollback behavior is used (true) or not (false).

• Type: true | false
• Default value: true
• Location: Add the property to the System Property [sys_properties] table.

**glide.rss.max_rows**

Controls the maximum number of records returned by the RSS Feed Generator.

• Type: integer
• Default value: 1000
• Location: Add the property to the System Property [sys_properties] table.

**glide.sc.reset_cascade**

If **true**, forces variable cascading when navigating between pages in an order guide.

- Type: true | false
- Default value: false
- Location: System Property [sys_properties] table

**glide.schedules.repeat_nth**

Controls how a schedule entry with **Repeats** set to **Monthly** and **Monthly Type** set to **Day of the Week** is defined. Choices are **Week** or **Day**. The **Week** option is defined as choosing a day of the month in the nth week selects the nth day of the month. The **Day** option is defined as choosing the nth day of the month selects the nth day of the month.

- Type: choice list
- Default value: day
- Location: System Property [sys_properties] table

**glide.schedules.fifth**

Controls how a schedule entry that selects the fifth occurrence of a day in month behaves in a month containing only four occurrences of the day. Choices are **Last**, **Next**, and **Strict**. The **Last** option selects the last (fourth) occurrence of the day. The **Next** option selects the first day of the next month. The **Strict** option skips the day completely. This property is valid only when the **glide.schedules.repeat_nth** property is set to **Day**.

- Type: choice list
- Default value: last
- Location: System Property [sys_properties] table

**glide.script.ccsi.ispublic**

Provides privacy control over client-callable script includes that are accessed by public pages. If **false**, all client-callable script includes are private.

- Type: true | false
- Default value: false
- Location: Add the property to the System Property [sys_properties] table.

**glide.script.log_level**

Controls the behavior of gs.log. Set this property to **none** to disable Glide script logging, or to **print** to save log data to the file system instead of the database. Use the default value **all** to save all Glide script logs to the database.

- Type: string
- Default value: all
- Location: Add the property to the System Property [sys_properties] table.

**glide.script_processor.admin**

Specifies the user role necessary to access the Scripts - Background module. To require administrators to elevate privileges to access the module, set the value to **security_admin**.

- Type: string
- Default value: admin
• Location: Add the property to the System Property [sys_properties] table.

**glide.script.vtable.log.debug**

Enables use of debug logs for remote table script definitions. Set this property to **true**. Prolonged use of this property can affect performance, so it is best to set its value to **false** when you finish a debugging session.

- Type: true | false
- Default value: false
- Location: Add the property to the System Property [sys_properties] table.

**glide.search.suggestions.enabled**

Set it to **true** (default) to enable search suggestions, or set it to **false** to disable search suggestions everywhere. For more information about search suggestions, see Enable search suggestions.

**glide.secondary.query.sysid**

Controls whether a secondary sort using sys_id as a sort key is automatically applied when sorting requested database records on a list. This property is useful when sorting records that have multiple records found for a single value of the primary sort key. Use this property to ensure that the [Next / Previous] buttons on forms display the proper record. If **false**, there is no secondary sort, therefore records with the same primary sort value are returned as they are found in the database and may be inconsistent.

- Type: true | false
- Default value: false
- Location: System Property [sys_properties] table

**glide.security.auto.resubmit.ajax**

Automatically resubmits timed-out Ajax requests.

- Type: true | false
- Default value: true
- Location: Add the property to the System Property [sys_properties] table.

**glide.security.checkacl.before.setvalue**

Controls how the high security setting glide.security.strict.updates processes ACLs. When **true**, the instance checks ACL rules for all columns before applying any updates to a row. When **false**, the instance applies ACL rules as each column is processed in alphabetical order. This behavior may result in one update preventing another update from occurring. For example, suppose that you create a custom ACL rule to prevent updates after a record is closed. If you attempt to close an incident and also add information to a custom resolution code field in the same update, the close action is applied first because it is controlled by the [incident.state] column and the custom field by the [incident.u_resolution_code] column. After the instance applies the close action, the custom ACL rule prevents further write updates to the row.

- Type: true | false
- Default value: true
- Location: Add the property to the System Property [sys_properties] table.

**glide.security.csrf.handle.ajax.timeout**

Handles errors for timed out Ajax requests.

- Type: true | false
• Default value: true
• Location: Add the property to the System Property [sys_properties] table.

**glide.security.csrf.strict.validation.mode**

Enforces strict validation on CSRF tokens so that users cannot resubmit a request if the CSRF token does not match.

• Type: true | false
• Default value: false
• Location: System Property [sys_properties] table
• Instance Security Hardening Settings: CSRF strict validation (instance security hardening)

**glide.security.diag_txns_acl**

Controls who can view the stats.do, threads.do, and replication.do pages. If **true**, only administrators or users from a known IP address are allowed to view the pages. If **false**, all users have access to the pages.

• Type: true | false
• Default value: false
• Location: Add the property to the System Property [sys_properties] table.
• Instance Security Hardening Settings: Performance monitoring (ACL) (instance security hardening)

**glide.security.disable_ui_pages_sysparm_client_script**

The system does not evaluate client scripts that are passed in URL parameters in UI pages. If you use URL parameters to load client scripts, you can add and disable this system property. Use this property only while you change the implementation to no longer depend on clients being passed in by URL parameters. Do not keep the system property disabled.

• Type: true | false
• Default value: true
• Location: Add the property to the System Property [sys_properties] table.

**glide.security.mime_type.aliasset**

Creates customized mime type alias sets. For example, `image/png=image/x-png`.

• Type: string
• Location: Add the property to the System Property [sys_properties] table.

**glide.security.granular.create**

Requires users to have write access on all individual fields on a table before they can create a record in that table.

• Type: true | false
• Default value: true
• Location: System Property [sys_properties] table

**glide.security.file.mime_type.validation**

Enables (**true**) or disables (**false**) MIME type validation for file attachments.

• Type: true | false
• Default value: false
• Location: System Property [sys_properties] table
• Instance Security Hardening Settings: Upload MIME type restriction (instance security hardening)
glide.security.strict_elevate_privilege

Forces all elevated roles to be treated equally for users with the administrator role. When enabled, administrators must explicitly, manually elevate themselves to any roles that are marked as elevated.

When disabled, administrators need only to manually elevate to the security_admin role. Other roles are automatically granted to administrators.

- Type: true | false
- Default value: true for new instances, false for upgraded instances
- Location: For new instances, this property is available on the System Property [sys_properties] table. For upgrades, Add the property to the System Property [sys_properties] table.

glide.service_portal.search_as_you_type_behavior

Select search suggestions (Suggestions) or type-ahead functionality (Typeahead). For more information about search suggestions, see Enable search suggestions.

glide.set_x_frame_options

Enables (true) or disables (false) the X-Frame-Options response header to SAMEORIGIN for all UI pages. The X-Frame-Options HTTP response header can be used to indicate whether a browser should be allowed to render a page in a <frame> or <iframe>. Set this property to true to avoid clickjacking attacks, by ensuring that CMS content cannot be embedded into other sites.

- Type: true | false
- Default value: true
- Location: System Property [sys_properties] table
- Instance Security Hardening Settings: X-Frame-Options: SAMEORIGIN (instance security hardening)

glide.short_poll_delay

(Chat plugin) Sets the short polling delay, in milliseconds, for XMPP requests. Polling is the method by which the browser gets information from the server to send instant messages in chat.

- Type: integer
- Default value: 1000 (1 second)
- Location: Social IT > Chat Administration > Properties

glide.shortened_journal_length

Sets the number of characters to display as a preview of journal input fields.

- Type: integer
- Default value: 512000
- Location: Add the property to the System Property [sys_properties] table.

glide.smtp.dateformat

Specifies the date format to use for outgoing email notifications

- Type: string
- Default value: date format [sys_user.date_format] listed in the user record of the email sender.
- Location: Add the property to the System Property [sys_properties] table.

glide.smtp.default_retry

Enables (true) or disables (false) resending email when an unknown SMTP error code is encountered. The instance recognizes only the SMTP error codes defined in the glide.smtp.defer_retry_ids property.
• Type: true | false
• Default value: true
• Location: **System Properties > Email**

### glide.smtp.defer_retry_ids
Specifies the comma-separated list of SMTP error codes that force the instance to resend email.

- Type: string
- Default value: 421,450,451,452
- Location: **System Properties > Email**

### glide.smtp.fail_message_ids
Specifies the comma-separated list of SMTP error codes that prevent the instance from resending email.

- Type: string
- Default value: 500,501,502,503,504,550,551,552,553,554
- Location: **System Properties > Email**

### glide.smtp.timeformat
Specifies the time format to use for outgoing email notifications.

- Type: string
- Default value: time format listed in email sender's user record [sys_user.time_format]
- Location: Add the property to the System Property [sys_properties] table.

### glide.soap.allow_null_numeric_output
When **true**, SOAP XML responses return an empty element for numeric fields with no value. When **false**, numeric fields with no value return a value of 0 in the SOAP response.

**Note:** The property **glide.wsdl.show_nillable** must be **true** to allow null values in SOAP responses.

- Type: true | false
- Default value: true
- Location: Add the property to the System Property [sys_properties] table.

### glide.soap.default_security_policy
Specifies the name of SOAP security policy the instance uses when enforcing Web Services Security (WSS) for inbound requests.

- Type: string
- Default value: default security policy
- Location: Add the property to the System Property [sys_properties] table.

### glide.soap.import_set_insert Serialized
Controls the processing of web service inserts. If **true**, the instance processes multiple simultaneous inserts one at a time (serially across nodes) to ensure an accurate transform. Serialized processing slows the speed at which the instance processes inserts. If **false**, multiple simultaneous inserts into an import set table result in simultaneous transforms that may produce duplicate target records due to the coalesce value being created at the same time.
**Note:** Set this value to `false` only to optimize performance when the related transform map does not have a coalesce value that may be present simultaneously.

- **Type:** true | false
- **Default value:** true
- **Location:** Add the property to the System Property [sys_properties] table.

### glide.soap.request_processing_timeout

Sets the maximum number of seconds that a SOAP request has to finish processing before the connection times out. This property computes a default value from the value of the property `glide.http.timeout` divided by 1000. There might be network infrastructure (such as proxy servers) in place that implements a shorter timeout. In this case, a socket timeout may occur unless this property is set to a shorter value. In general, you should set this property to a value several seconds less than the shortest socket inactivity timeout in effect anywhere in the network path between the client application and the ServiceNow instance.

- **Type:** integer
- **Default value:** 175 (value of `glide.http.timeout` divided by 1000)
- **Location:** System Property [sys_properties] table

### glide.source_control.checksum_required

This property allows you to enable optional checksum validations and sanitizations. When set to `true`, continues to throw an error if the checksum validation of application files fails. This action prevents application developers on your instance from importing application files from source control that have been modified outside of an instance.

- **Type:** true | false
- **Default value:** false
- **Location:** System Property [sys_properties] table

### glide.source_control.checksum_quick_install

When set to `true`, bypasses the sanitization step(s) if the checksum matches. This action prevents an application developer from waiting for validation/sanitization steps to be processed if application files linked to a source control repository outside of your instance weren't modified.

- **Type:** true | false
- **Default value:** true
- **Location:** System Property [sys_properties] table

### glide.source_control.default_branch_name

Sets the default GIT repository branch to work in for application files linked to source control.

- **Type:** string
- **Default value:** sn_instances/<instance_name>
- **Location:** System Property [sys_properties] table

### glide.spell.dictionary.en

Sets the spell checker dictionary used in the system for English users. Dictionaries are available for Brazilian Portuguese (pb.dic), Czech (cs.dic), Dutch (nl.dic), English US (en.dic), English UK (en_uk.dic), Estonian (et.dic), Finnish (fi.dic), French (fr.dic), German (de.dic), Hebrew (he.dic), Hungarian (hu.dic), Italian (it.dic), Polish (pl.dic), Portuguese (pt.dic), Russian (ru.dic), Spanish (es.dic), and Thai (th.dic).

- **Type:** choice list
- **Default value:** en.dic (English US)
• Location: System Property [sys_properties] table

**glide.spell.dictionary.max_matches**

Specifies the maximum number of spelling errors that the spell-check should detect. By default, spell-check finds only 10 spelling errors. The instance ignores any additional errors after reaching the maximum value.

• Type: integer
• Default value: 10
• Location: System Property [sys_properties] table.

**glide.sys.activity_using_audit_direct**

[Not Supported] Controls whether the record’s history is generated using the Audit table (true) or not (false). [Required] Set the value to false to generate history with History Sets.

• Type: true | false
• Default value: false
• Location: System Property [sys_properties] table

**glide.sys.audit_inserts**

Specifies whether the Audit table audits inserts (true) or not (false).

• Type: true | false
• Default value: false
• Location: System Property [sys_properties] table

**glide.sys.date_format**

System date format for all users unless overridden in the user record.

• Type: date format
• Default value: yyyy-MM-dd
• Location: System Properties > Basic Configuration U116

**glide.sys.default.tz**

System timezone for all users unless overridden in the user's record.

• Type: timezone
• Default Value: none
• Location: System Properties > Basic Configuration U116

**glide.sys.domain.domain_change_notify**

Domain legacy

• Type: true | false
• Default value: true
• Location: System Property [sys_properties] table

**glide.sys.domain.no_change_roles**

Domain legacy

• Type: string
• Default value: This field should be left empty.
• Location: System Property [sys_properties] table

**glide.sys.domain.use_record_domain**

Domain legacy
- Type: true | false
- Default value: true
- Location: System Property [sys_properties] table

**glide.sys.domain.use_record_domain_for_client_scripts**

Domain legacy
- Type: true | false
- Default value: false
- Location: System Property [sys_properties] table

**glide.sys.time_format**

System time format for all users unless overridden in the user's record.
- Type: time format
- Default Value: HH:mm:ss
- Location: System Properties > Basic Configuration UI16

**glide.sys_reference_row_check**

Specifies whether the script conditions of Access Control Rules apply to a table's reference fields (true) or not (false).
- Type: true | false
- Default value: false
- Location: Add the property to the System Property [sys_properties] table.

**glide.template.max_context**

Specifies the maximum number of templates displayed in a form's context menu. If more than this number are available, users can click Apply Template on the context menu to open the reference list of templates.
- Type: integer
- Default value: 15
- Location: System Property [sys_properties] table

**glide.transform.reuse_coalesce_field_value**

If true, avoid re-evaluation of coalesce scripts to get the values.
- Type: true | false
- Default value: true
- Location: Add the property to the System Property [sys_properties] table.

**glide.translate.learn**

Enables (true) or disables (false) adding the current language suffix to UI elements such as labels and messages. Enabling the language suffix assists with translating new customizations.
- Type: true | false
• Default value: false
• Location: Add the property to the System Property [sys_properties] table.

**glide.ts.index.attachment.debug**

If `true`, enables log messages for exceptions that occur when indexing attachments. You can leave this property enabled during normal operations to capture stack trace information about any exceptions.

• Type: true | false
• Default value: false
• Location: Add the property to the System Property [sys_properties] table.

**glide.ts.index.attachment.list_terms.debug**

If `true`, the system logs all indexed terms when an attachment is indexed.

For optimal performance, set this property to `false` during normal operations. Only enable this property when you are actively debugging an issue.

• Type: true | false
• Default value: false
• Location: Add the property to the System Property [sys_properties] table.

**glide.ts.reindex.sys_metadata.after.upgrade**

If `true`, the system automatically reindexes the sys_metadata table after an upgrade, without noticeable performance impact. To disable automatic reindexing, set the value to `false`.

• Type: true | false
• Default value: true
• Location: Add the property to the System Property [sys_properties] table.

**glide.ui.activity.displayname**

Specifies whether the activity formatter shows `name` values (true) or `user_name` values (false).

• Type: true | false
• Default value: false
• Location: Add the property to the System Property [sys_properties] table.

**glide.ui.activity.email_roles**

Specifies the list of roles (comma-separated) that can view email in the Activity Formatter.

• Type: string
• Default value: itil
• Location: Add the property to the System Property [sys_properties] table.

**glide.ui.activity.email.use_display**

Specifies whether to display the email address or the user IDs (display value of the User table) in email headers (`true`) or not (`false`). If `true`, the instance searches for a user record with a matching email address. If the instance cannot find a matching user record, it displays the email address.

• Type: true | false
• Default value: false
• Location: Add the property to the System Property [sys_properties] table.
glide.ui.activity_stream.form_button
Removes the activity stream button from forms.
- Type: true | false
- Default value: true
- Location: Add the property to the System Property [sys_properties] table.

glide.ui.activity_stream.list_button
Removes the activity stream button from lists.
- Type: true | false
- Default value: true
- Location: Add the property to the System Property [sys_properties] table.

glide.ui.activity_stream.page_size
Size of pages for UI16 form activity stream. A value of 0 means no paging.
- Type: integer
- Default value: 0
- Location: Still appears in the System Properties [sys_properties] table, but is no longer available.

glide.ui.activity_stream.scale_animated_gifs
Creates a thumbnail of animated .gif files. The maximum dimensions are 525 px width and 350 px height. The animation is not preserved in the thumbnail, but previewing the image displays the animation at its original size.
- Type: true | false
- Default value: false
- Location: System Property [sys_properties] table

glide.ui.activity_stream.scale_images
Creates a thumbnail of large images to display in the activity stream. The maximum dimensions are 525 pixels wide and 350 pixels high. If the user clicks the image or attachment, the preview is at full size.
- Type: true | false
- Default value: true
- Location: System Property [sys_properties] table

glide.ui.activity_stream.style.comments
Changes the color of the left bar in activity stream comments in UI16.
- Type: color entry, either a name, such as blue or a code, such as #0000FF.
- Default value: transparent
- Location: System Property [sys_properties] table

glide.ui.activity_stream.style.work_notes
Changes the color of the left bar in activity stream work notes in UI16.
- Type: color entry, either a name, such as blue or a code, such as #0000FF.
- Default value: gold
- Location: System Property [sys_properties] table
`glide.ui.activity.style.comments`
Changes the background color of the activity stream comments in UI15.
- Type: string
- Default value: background-color: background-color: WhiteSmoke
- Location: System Property [sys_properties] table

`glide.ui.activity.style.work_notes`
Changes the background color of the activity stream work notes in UI15.
- Type: string
- Default value: background-color: LightGoldenRodYellow
- Location: System Property [sys_properties] table

`glide.ui.allow.field.dependency.for.templates`
Checks dependency for choice fields at the time of applying template, preventing invalid values to be set to the dependent field. For example, a subcategory field which depends on category field.
- Type: true | false
- Default value: true
- Location: System Property [sys_properties] table

`glide.ui.allow_deep_html_validation`
Allows administrators to prevent users from saving invalid HTML in a journal field.
- Type: true | false
- Default value: false
- Location: System Property [sys_properties] table

Add the property to the System Property [sys_properties] table.

`glide.ui.attachment.force_download_all_mime_types`
Forces download of all MIME attachment files.
- Type: true | false
- Default value: true for new instances, false for upgraded instances
- Location: System Property [sys_properties] table
- Instance Security Hardening Settings: Force Download MIME types (instance security hardening)

`glide.ui.audit_deleted_tables`
Comma-separated list of system tables for which the audit history tracks deletions.
- Type: string
- Default value: sys_user, sys_user_group, sys_user_role, sys_user_has_role, sys_user_grmember, sys_group_has_role, sys_security_acl_role
- Location: System Property [sys_properties] table

`glide.ui.auto.recovery`
Allows users to recover unsaved changes while working in the Studio.
- Type: true | false
- Default value: true
• Location: **Auto Recovery > Properties**

**glide.ui.auto.recovery.exclude.field.types**
Comma-separated list of field types to exclude from automatic recovery.

• Type: string
• Default value: none

• Location: **Auto Recovery > Properties**

**glide.ui.auto.recovery.unsupported.field.types**
Comma-separated list of field types no supported for automatic recovery.

• Type: string
• Default value: password,password2,glide_encrypted,video,user_image,image

**glide.ui.auto.recovery.unsupported.tables**
Comma-separated list of tables to exclude from automatic recovery.

• Type: string
• Default value: v_ws_editor

• Location: **Auto Recovery > Properties**

**glide.ui.auto_req.extend.session**
If true, enables the user to extend their user session by selecting a homepage refresh time. If false, it enforces session timeout. The session timeout value is ignored when the user specifies an automatic refresh value.

For example, if the user selects 5 minutes for automatic homepage refresh, the session is renewed every five minutes. By adding this property and setting the value to false, administrators can force the user session to time out even if the user page refreshes every x number of minutes. The user session times out after the value specified in the session timeout, plus the selected refresh value. This property takes effect when the Remember me check box is not selected for the user. Tablet and mobile devices do not support this feature.

• Type: true | false
• Default value: true

• Location: Add the property to the System Property [sys_properties] table.

**glide.ui.buttons_bottom**
Controls whether UI actions appear at both the bottom and top of the form (true) or only at the top (false). This property only works in a deprecated version of the UI.

• Type: true | false
• Default value: false

• Location: System Property [sys_properties] table

**glide.ui.cert_task_activity.fields**
Defines which journal field is the task activity field.

• Type: string
• Default value: work_notes

• Location: Add the property to the System Property [sys_properties] table.

**glide.ui.chart.bar.horiz.max_col_slant_labels**
Sets the maximum number of columns in a horizontal bar chart before slanting (angling) the labels.

- **Type**: integer
- **Default value**: 5
- **Location**: Add the property to the System Property [sys_properties] table.

**glide.ui.chart.height**

Specifies the height of a chart in pixels.

- **Type**: integer
- **Default value**: 300
- **Location**: Add the property to the System Property [sys_properties] table.

**glide.ui.chart.pie.labels**

Enables (true) or disables (false) labels on pie chart slices.

- **Type**: true | false
- **Default value**: true
- **Location**: Add the property to the System Property [sys_properties] table.

**glide.ui.chart.pie.labels.max_items**

Sets the maximum number of pie chart slice values that can be returned to display their labels.

- **Type**: integer
- **Default value**: 8
- **Location**: Add the property to the System Property [sys_properties] table.

**glide.ui.clickthrough.popup**

- For reference fields, enables (true) or disables (false) display of the pop-up diamond icon for reference fields, and opening a new window when clicking the icon.
- For document ID fields, enables (true) or disables (false) displaying the information icon and opening a pop-up window with the document’s form. To learn more Document ID field.

**Note**: Related lists do not appear on forms opened in the pop-up window.

- **Type**: true | false
- **Default value**: false
- **Location**: System Property [sys_properties] table

**glide.ui.clickthrough.replace**

Enables (true) or disables (false) both the pop-up and click-through icons for reference fields.

- **Type**: true | false
- **Default value**: false
- **Location**: System Property [sys_properties] table

**glide.ui.concourse.onmessage_enforce_same_origin_whitelist**

Inclusion list of trusted origins for propagated messages (sent via `window.postMessage()` Web API) in the UI. Origins must include scheme and can be separated by comma, space, or new line. For example: `https://`

- Type: string
- Default: none
- Location: System Property [sys_properties] table

**glide.ui.concourse.onmessage_enforce_same_origin**

Enforces an origin check before propagating a message (sent via `window.postMessage()` Web API) in the UI. If set to `true`, only URLs from ServiceNow are allowed to propagate messages. If set to `false`, all URLs included in `glide.ui.concourse.onmessage_enforce_same_origin_whitelist` can propagate messages in the UI.

- Type: true | false
- Default value: true
- Location: System Property [sys_properties] table

**glide.ui.date_format.first_day_of_week**

Specifies which day of the week that weeks start on for calendar reports (1=Sunday, 2=Monday...).

- Type: integer
- Default value: 1
- Location: System Property [sys_properties] table

**glide.ui.date_picker.first_day_of_week**

Specifies the first (leftmost) day of the week for the date and date/time picker (1=Sunday, 2=Monday...).

- Type: integer
- Default value: 1
- Location: System Property [sys_properties] table

**glide.ui.default.applications**

Comma-separated list of application names that open by default in the navigation pane when nothing is opened via user preferences. If the property is specified and is blank, no applications are opened in the navigation pane when no applications are opened via user preferences. If the property is not specified, the first application that is authorized for the user opens if no applications are opened via user preferences.

- Type: string
- Default value: first authorized application for the user
- Location: Add the property to the System Property [sys_properties] table.

**glide.ui.dirty_form_support**

Enables (true) or disables (false) display of a confirmation message when a form has unsaved changes and the user leaves the form through any means except a submit (such as using the green back arrow, any form button, or other). This property is not supported in Safari.

- Type: true | false
- Default value: true
- Location: Add the property to the System Property [sys_properties] table.

**glide.ui.encode_module_uri**

Enables (true, the default) or disables (false) encoding of module URIs in the navigation pane. For information about how ServiceNow encodes module URIs, see Encoding module URIs.
**glide.ui.doctype**

Enables or disables the UI15 interface.

- **Type:** true | false
- **Default value:** true
- **Location:** System Property [sys_properties] table

**glide.ui.filter.first_day_of_week**

Identifies the first day of the calendar week for the company. By default, the start of the week is Monday, meaning that the calendar week begins with Monday and ends with Sunday. To change this behavior, add the property **glide.ui.filter.first_day_of_week** to the instance as an integer property. Set the value to the integer corresponding with the day of the week that the calendar begins on, where 1 is Sunday, 2 is Monday, and so on. The function impacts all charts and calculations where the day of the week is used as a parameter.

- **Type:** integer
- **Default value:** 2
- **Location:** Add the property to the System Property [sys_properties] table.

**glide.ui.first.field.reference**

Enables (true) or disables (false) having the first column in a list always link to the underlying record, even if it is a reference field. For example, if the first column on an Incident list is Assigned to, that value links to the Incident if this property is set to true.

- **Type:** true | false
- **Default value:** false
- **Location:** Add the property to the System Property [sys_properties] table.

**glide.ui.form_annotations**

Enables (true) or disables (false) form annotations, which allow you to add Custom, Section Separator, and Line Separator to a form.

- **Type:** true | false
- **Default value:** true
- **Location:** System Property [sys_properties] table

**glide.ui.form_multiple_splits**

Enables (true) or disables (false) multiple splits and end splits in the form layout configuration slushbucket.

- **Type:** true | false
- **Default value:** true
- **Location:** System Property [sys_properties] table

**glide.ui.gauge.view**

Defines which view you want to be the default for homepage gauges.

- **Type:** string
- **Default value:** portal
- **Location:** System Property [sys_properties] table

**glide.ui.glide_list.start.locked**

Controls whether a glide_list (like the watch list) starts out locked (true) or unlocked (false) on a form.
• Type: true | false
• Default value: true
• Location: System Property [sys_properties] table

**glide.ui.goto_use_contains**
Controls whether the Go to navigation performs a "contains" query (true) or a "greater than" query (false) by default.

• Type: true | false
• Default value: false
• Location: Add the property to the System Property [sys_properties] table.

**glide.ui.homepage.parallel**
Enables (true) or disables (false) use of parallel rendering.

• Type: true | false
• Default value: true
• Location: System Property [sys_properties] table

**glide.ui.homepage.parallelism**
Sets the maximum number of threads that should cooperate on rendering any given homepage.

• Type: integer
• Default value: 2
• Location: System Property [sys_properties] table

**glide.ui.homepage.preview**
Enables (true) or disables (false) displaying the preview icon for lists on the homepage.

• Type: true | false
• Default value: true
• Location: System Property [sys_properties] table

**glide.ui.html.editor**
Specifies which HTML field editor to use, TinyMCE or htmlArea (legacy).

• Type: string
• Default value: tinymce
• Location: System Properties > UI Properties

**glide.ui.html.editor.extended_valid_elements**
Defines which elements remain in the TinyMCE text when the editor saves. This functionality can be useful to add or override specific elements that should be kept.

- Type: string
- Default value: blank
- Location: System property [sys_properties] table

**glide.ui.html.editor.toolbar.line1**

Configures the editing toolbar (first line) for HTML fields when TinyMCE is enabled. The spellchecker tool is not supported in UI16 or UI15.

- Type: string
- Location: System Properties > UI Properties

**glide.ui.html.editor.toolbar.line2**

Configures the editing toolbar (second line) for HTML fields when TinyMCE is enabled. The spellchecker tool is not supported in UI16 or UI15.

- Type: string
- Location: System Properties > UI Properties

**glide.ui.html.editor.v4.paste.html_import**

Controls how content being pasted from sources other than Microsoft Word is filtered. This includes content copied from TinyMCE itself.

- Type: choice list
- Default value: clean
- Location: System Property [sys_properties] table

**glide.ui.html.image.allow_url**

Enables (true) or disables (false) uploading an image via URL from HTML Fields.

- Type: true | false
- Default value: false
- Location: System Property [sys_properties] table

**glide.ui.html.editor.remove_trailing_brs**

Specifies whether an empty line containing a <br> tag is converted to a <div>&nbsp;</div> tag for TinyMCE HTML fields. If true, the tag is converted. If false, the tag is left as <br>.

- Type: true | false
- Default value: true
- Location: System Properties > UI Properties

**glide.ui.html.toolbar**

Configures the editing toolbar for HTML fields.

- Type: string
- Default value: list of buttons
- Location: System Properties > UI Properties
**glide.ui.incident_activity.fields**

Defines what fields are visible in the activity formatter. If the activities are customized, the system updates this property automatically.

- Type: string
- Default value: list of fields
- Location: **System Properties > UI Properties**

**glide.ui.incident_activity.max_addresses**

Specifies the maximum number of addresses to list in an email audit record. If the number of addresses exceeds this limit, the instance truncates the list after the maximum value and displays an ellipsis character (...).

- Type: string
- Default value: 5
- Location: **Add the property** to the System Property [sys_properties] table.

**glide.ui.incident_alert_activity.fields**

Incident communication plan activity formatter fields — the list of fields tracked from the Incident Communication Plan form in the activity formatter.

- Type: string
- Default value: opened_by, work_notes, comments, severity, estd_distruption_time, actual_disruption_time
- Location: **System Property [sys_properties] table**

**glide.ui.journal.use_html**

Specifies whether TinyMCE is available for journal fields (true) or not (false).

- Type: true | false
- Default value: false

**glide.ui.js_error_notify**

Displays client script errors to users with the **client_script_admin** role. Also displays a generic error message to other users who encounter a client script error.

- Type: true | false
- Default value: true
- Location: **System Properties > All Properties**

**glide.ui.label.enable**

Enables (true) or disables (false) using labels, such as Most Active, Most Recent, or user-created.

- Type: true | false
- Default value: true
- Location: System Property [sys_properties] table

**glide.ui.m.clear_pasteboard_when_backgrounded**

Clears the copy/paste clipboard when the application enters the background.

- Type: true | false
- Default value: false
• Location: Add the property to the System Property [sys_properties] table. In Categories, add the mobile_post_auth category.

**glide.ui.max_calendar_duration**

Maximum number of days that a single calendar report entry can display.

• Type: integer
• Default value: 90
• Range of possible values: 90 to 400
• Location: System Property [sys_properties] table

**glide.ui.max_calendar_records**

Maximum number of records saved in a calendar report.

• Type: integer
• Default value if the property is not configured: 10,000
• Location: System Property [sys_properties] table

**glide.ui.m_agents**

Comma-separated list of browser agents considered as mobile browsers for the Smartphone Interface. These browsers are directed to the mobile pages instead of the full browser pages.

• Type: string
• Default value: iphone,android_phone,IEMobile,Windows Phone,iPod,Windows CE,BlackBerry,BB10
• Location: System Property [sys_properties] table

**glide.ui.max_ref_dropdown**

Maximum number of records for a reference field that is displayed as a choice list. If the number of available records is greater than this value, the field appears as a reference field, not as a choice list.

• Type: integer
• Default value: 25
• Location: System Property [sys_properties] table

**glide.ui.mentions.default_limit**

Number of users with same name displayed in Activity Stream Compose editor. When set to true, the default limit takes in a number which determines how many users with the same name are displayed.

• Type: string
• Default value: true
• Location: System Property [sys_properties] table

**glide.ui.mobile_agents**

Comma-separated list of browser agents considered as mobile browsers for the Legacy Smartphone Interface. These browsers are directed to the mobile pages instead of the full browser pages.

• Type: string
• Default value: iPod,Windows CE,BlackBerry,Android,Opera Mini,IEMobile,Windows Phone,iphone
• Location: System Property [sys_properties] table

**glide.ui.nav.stripe.select.maxchars**
Numerical character limit for list menu choices within the nav stripe. The nav stripe appears at the top of the page when using UI11.

- Type: integer
- Default value: none
- Location: Add the property to the System Property [sys_properties] table.

**glide.ui.reference.readonly.clickthrough**

Enables (true) or disables (false) reference pop-ups on read-only reference fields. Reference pop-ups and click-throughs are hidden by default if a client script, UI policy, or ACL makes the field read-only. Being able to see or click through to the target record is unrelated to the reference field being writable.

If false, the administrator can override the system setting for a specific field by adding the `readonly.clickthrough=true` attribute to the dictionary entry.

- Type: true | false
- Default value: false
- Location: System Properties > UI Properties

**glide.ui.remember_view**

Enables (true) or disables (false) use of user preferences for the last view.

- Type: true | false
- Default value: true
- Location: System Property [sys_properties] table

**glide.ui.remember.me.default**

Controls whether the Remember me check box is selected (true) or cleared (false) by default.

- Type: true | false
- Default value: true
- Location: System Property [sys_properties] table

**glide.ui.report.extend_calendar_choices**

Controls which field styles are applied during calendar highlighting. If false, field styles in only the Task table are used. If true, the calendar first uses field styles from the table that the report is based on. If no applicable styles exist in that table, the calendar uses field styles from the Task table.

- Type: true | false
- Default value: true
- Location: System Property [sys_properties] table

**glide.ui.report.old_report_builder**

Enables (true) or disables (false) use of the old report builder UI.

- Type: true | false
- Default value: false
- Location: Add the property to the System Property [sys_properties] table.

**glide.ui.section508**

Enables (true) or disables (false) rendering of alternate text in place of images.
• Type: true | false
• Default value: false
• Location: System Properties > UI Properties

**glide.ui.show_live_feed_activity**
Enables (true) or disables (false) live feed for a record in the activity formatter.

• Type: true | false
• Default value: false
• Location: System Properties > UI Properties

**glide.ui.show_template_bar**
Controls whether the template bar can be displayed on the specified table. For example:
`glide.ui.show_template_bar.incident = false`.

• Type: true | false
• Default value: true
• Location: Add the property to the System Property [sys_properties] table.

**glide.ui.session_timeout**
Sets the session timeout, in minutes.

• Type: integer
• Default value: 30
• Location: System Property [sys_properties] table

**glide.ui.stream_icon**
Toggles the displaying of the activity stream button on the specified table. For example:
`glide.ui.stream_icon.hr_case = true`.

• Type: true | false
• Default value: false

**glide.ui.syntax_editor.context_menu**
Enables disables the context menu in script editor.

• Type: true | false
• Default value: true
• Location: System Property [sys_properties] table

**glide.ui.syntax_editor.linter.eslint_config**
Defines linting configurations using the ESLint utility.

• Type: string
• Default value: All recommended ESLint rules are enabled, except no-undef, no-unused-vars, no-empty, and semi.
• Location: System Property [sys_properties] table

**glide.ui.table.labels**
Controls whether the system uses verbose labels for table names (true) or literal table names (false).

• Type: true | false
• Default value: true
• Location: System Property [sys_properties] table

**glide.ui.tablet_enabled**

Enables (true) or disables (false) the tablet UI.

• Type: true | false
• Default value: true
• Location: System Properties > Tablet UI Properties

**glide.ui.tablet_agents**

Uses the tablet UI if one of the specified strings (comma-separated) appears in the browser user_agent header.

• Type: string
• Default value: ipad,android_tablet
• Location: System Properties > Tablet UI Properties

**glide.ui.tablet.title**

Displays the specified text as a brief page title for tablet UI.

• Type: string
• Default value: ServiceNow
• Location: System Properties > Tablet UI Properties

**glide.ui.tablet.title.ios_webapp**

Displays the specified text as the default home screen icon label used in iOS version 6 and later.

• Type: string
• Default value: ServiceNow
• Location: System Properties > Tablet UI Properties

**glide.ui.task.insert**

Enables (true) or disables (false) the use of Insert and Insert and Stay options on tables derived from Task (such as Incident, Change, and Problem).

• Type: true | false
• Default value: false
• Location: System Property [sys_properties] table

**glide.ui.textarea.character_counter**

When true, displays a count of available characters for journal and multi-line text fields.

• Type: true | false
• Default value: false
• Location: System Property [sys_properties] table

**glide.ui.textarea_initial_rows**

Sets the number of rows initially displayed for multiline form elements. When the element is selected for editing, it is expanded. Set this value to 0 or blank to ignore this property. This functionality is used to conserve space on a form when multiline elements take up too much space.
**glide.ui.update_on_iterate**
Controls whether updates are saved (true) or discarded (false) when a user clicks the blue arrows on a form.
- Type: true | false
- Default value: false
- Location: System Property [sys_properties] table

**glide.ui.ui_policy_debug**
Enables (true) or disables (false) logging of UI policy processing in the JavaScript debug window
- Type: true | false
- Default value: false
- Location: Add the property to the System Property [sys_properties] table.

**glide.ui.user_cookie.life_span_in_days**
Sets the expiration time period for the 'remember me' cookie.
- Type: integer
- Default value: 15 (days)

**Note:** When a user accesses an instance with 'remember me' enabled, the access resets the cookie expiration period until the maximum (glide.ui.user_cookie.max_life_span_in_days) life span limit is reached.
- Location: System Property [sys_properties] table

**glide.ui.user_cookie.max_life_span_in_days**
Sets a maximum cap for the glide.ui.user_cookie.life_span_in_days cookie to expire before forcing a user to re-authenticate into the instance.
- Type: integer
- Default value: 30 (days)

**Note:** Maximum value 30.
- Location: System Property [sys_properties] table

**glide.ui.welcome.profile_link**
Enables (true) or disables (false) allowing users to click their name in the welcome message and see their user profile.
- Type: true | false
- Default value: In new instances true. In existing instances false.
- Location: System Property [sys_properties] table
glide.ui11.show_switch_link

This property only affects a deprecated version of the UI. It is no longer supported. Displays (true) or hides (false) a banner link for switching between the UI11 and legacy interfaces.

- Type: true | false
- Default value: true
- Location: System Property [sys_properties] table

glide.update.suppress_update_version

Comma-separated list of tables for which updates are not tracked in the Versions [sys_update_version] table. You cannot compare and revert versions for tables in this list.

- Type: string
- Default value: sys_user,sys_import_set_row
- Location: Add the property to the System Property [sys_properties] table.

glide.user.default_password

Default password for new users created from incoming email. Users must reset the password at first login.

- Type: string
- Default value: password
- Location: System Properties > Email
- Instance Security Hardening Settings: Set complex default password (instance security hardening)

glide.userauthgate.extauth.check

Enables (true) or disables (false) the UserAuthenticationGate checks for both external and internal authentication mechanisms.

- Type: true | false
- Default value: false
- Location: System Property [sys_properties] table

glide.user.trusted_domain

Comma-separated list of trusted domains for which the instance automatically creates a guest user based on incoming emails. Use an asterisk (*) to trust all domains. If an email is not from a trusted domain, the instance processes the inbound email as a “guest user” but does not create a guest user in the instance.

- Type: string
- Default value: *
- Location: System Properties > Email

glide.workflow.model.cache.max

Maximum number of models held in the workflow cache. You must restart the instance after changing this property to apply the change.

- Type: integer
- Default value: 300
- Location: Workflow > Properties

glide.wsdl.definition.use_unique_namespace
Enables (true) or disables (false) use of a unique WSDL namespace value when publishing a ServiceNow table through web services. If true, the WSDL target namespace is www.service-now.com/<table name>.

- Type: true | false
- Default value: false
- Location: Add the property to the System Property [sys_properties] table.

**glide.wsdl.maximum_hierarchy**

Maximum number of hierarchical levels returned in a WSDL when hierarchical SOAP web service is enabled. This property has a maximum value of 3.

- Type: integer
- Default value: 3
- Location: Add the property to the System Property [sys_properties] table.

**glide.wsdl.show_nullable**

Enables (true) or disables (false) allowing a WSDL element to be valid if it has no element content despite a {content type} which would otherwise require content.

- Type: true | false
- Default value: false
- Location: Add the property to the System Property [sys_properties] table.

**glide.ws.use_row_lock**

If true, avoid using the current web service lock that applies before running the transform. Use the row lock that applies after the OnStart method.

- Type: true | false
- Default value: false
- Location: Add the property to the System Property [sys_properties] table.

**glide.xmlhttp.excessive**

Sets the number of items visible in the Available half of a many-to-many or one-to-many collection box.

- Type: integer
- Default value: 100
- Location: Add the property to the System Property [sys_properties] table.

**glide.xmlprocessor.use_unload_format**

Enables (true) or disables (false) unloading the XML using the display_value format. To unload using this format, add the parameter useUnloadFormat=true to the request URL.

- Type: true | false
- Default value: false
- Location: Add the property to the System Property [sys_properties] table.

**google.maps.auto_close**

If true, automatically closes the current info window before opening a new one. Clear the check box to enable multiple pop-up windows to remain open at once.

- Type: true | false
- Default value: true
• Location: System Properties > Google Maps

google.maps.client

Client ID for Google Maps API for Business. This client ID authorizes production use of Google Maps API for Business. By default, this ID is provided by ServiceNow. ServiceNow may require you to purchase a separate Client ID based on your usage.

• Type: string
• Default value: gme-servicenow
• Location: System Properties > Google Maps

google.maps.key

Map key from Google, tied to the URL of the server. This key is the private key authorizing development use of Google Maps.

• Type: string
• Default value: empty
• Location: System Properties > Google Maps

google.maps.latitude

Starting latitude of the map. This value determines the starting latitude displayed in Google Maps.

• Type: string
• Default value: 36.008522
• Location: System Properties > Google Maps

google.maps.longitude

Starting longitude of the map. This value determines the starting longitude displayed in Google Maps.

• Type: string
• Default value: -95.221764
• Location: System Properties > Google Maps

google.maps.max_items

Maximum number of items to display on the map. This setting determines how many icons can be displayed on a map.

• Type: integer
• Default value: 500
• Location: System Properties > Google Maps

google.maps.table

Table used by the map. This setting names the table containing the name, longitude, and latitude fields.

• Type: string
• Default value: cmn_location
• Location: System Properties > Google Maps

google.maps.zoom

Starting zoom level of the map (1 is the lowest).

• Type: integer
• Default value: 4
• Location: **System Properties > Google Maps**

**help.base.default**

(Context-Sensitive Help plugin) Sets the base URL for help contexts in which ServiceNow wiki is **false** and an absolute URL is not specified.

- Type: string
- Default value: `http://docs.servicenow.com/?context=`
- Location: System Property [sys_properties] table

**help.base.servicenow**

(Context-Sensitive Help plugin) Sets the base URL for help contexts in which ServiceNow wiki is **true**

- Type: string
- Default value: `http://docs.servicenow.com/?context=`
- Location: System Property [sys_properties] table

**mid.server.rba_debug_powershell**

Enables probe-level debugging for PowerShell probes. With this property enabled, PowerShell probes write detailed activity information to the MID Server log.

- Type: true | false
- Default value: false
- Location: **Orchestration > MID Server Properties**

**mid.version.override**

Sets an override condition for the current version for all MID Servers in your environment. For more information on version control, see **MID Server version control properties**.

- Type: string
- Default value: none (If this property is left empty, the MID Servers get their version information from the mid.buildstamp property.)
- Location: Add the property to the System Property [sys_properties] table.

**par_vis_config.data_source.can_select_indicator**

 Specifies roles (comma-separated) which can select indicators as data sources from the Data Visualization configuration panel. If empty, all users can select the indicator sources that they have access to.

- Type: string
- Default value: empty
- Location: System Property [sys_properties] table

**par_vis_config.live_refresh_rate_min_value**

Specifies the minimum interval in seconds for the **Live refresh rate** setting in the Data Visualization configuration. If set, a user can still set an empty or 0 value.

- Type: integer
- Default value: 30 (seconds)
- Location: System Property [sys_properties] table
password_reset.activity_monitor.incident_threshold

Specifies the maximum number of lockouts before an alert is issued.

- Type: integer
- Default value: 10 (lockouts)
- Location: System Property [sys_properties] table

password_reset.activity_monitor.incident_window

Specifies the amount of time that is used for recording and counting the number of user lockouts.

- Type: integer
- Default value: 60 (minutes)
- Location: Password Reset > Properties

password_reset.captcha.ignore

Enables and disables CAPTCHA functionality.

The password reset application uses Google re-CAPTCHA as the default CAPTCHA service. To use the base system CAPTCHA, change the password_reset.captcha.google.enabled system property to false.

- Type: true | false
- Default value: false
- Location: Password Reset > Properties

password_reset.qa.num_enroll

Specifies the number of questions a user must select and answer to be enrolled in the password reset program.

**Note:** This security question property can be overridden by adding a value for the num_enroll parameter in a security question verification.

- Type: integer
- Default value: 5 (questions)
- Location: Password Reset > Properties

password_reset.qa.num_reset

Specifies the number of questions a user must answer to verify their identity during the password reset process.

**Note:** This security question property can be overridden by adding a value for the num_reset parameter in a security question verification.

- Type: integer
- Default value: 3 (questions)
- Possible values: integers that are less than the number specified for the num_enroll property.
- Location: Password Reset > Properties

password_reset.request.max_attempt

Specifies the number of password reset attempts a user has before they are locked out for a period determined by the value in max_attempt_window.

- Type: integer
- Default value: 3 (attempts)
• Location: **Password Reset > Properties**

**password_reset.request.max_attempt_window**

Specifies how long a user is locked out or prevented from changing their password after trying the maximum number of times.

- Type: integer
- Default value: 1440 (minutes)
- Location: **Password Reset > Properties**

**password_reset.request.retry_window**

Specifies the length of time before the count for password reset attempts refreshes.

- Type: integer
- Default value: 1440 (minutes)
- Location: **Password Reset > Properties**

**password_reset.request.success_window**

Specifies how long a user is locked out after they have successfully reset their password.

- Type: integer
- Default value: 10 (minutes)
- Location: **Password Reset > Properties**

**password_reset.sms.default_complexity**

Specifies the number of characters in the SMS code that are required for a user to reset their password.

> **Note:** This SMS code property can be overridden by adding a value for the complexity parameter in an SMS code verification.

- Type: integer
- Default value: 4 (digits)
- Location: **Password Reset > Properties**

**password_reset.sms.expiry**

Specifies the amount of time, in minutes, until the SMS code sent to the user expires.

> **Note:** This SMS code property can be overridden by adding a value for the expiry parameter in an SMS code verification.

- Type: integer
- Default value: 5 (minutes)
- Location: **Password Reset > Properties**

**password_reset.sms.max_per_day**

Specifies the maximum number of SMS codes that are sent to a user within one 24-hour period. When a user clicks the **Send Verification Code** button, the 24-hour period begins.
**password_reset.sms.pause_window**

Specifies the amount of time to pass before another SMS code can be sent to a user.

- Type: integer
- Default value: 2 (minutes)
- Location: Password Reset > Properties

**password_reset.wf.refresh_rate**

Specifies how often to check status of the workflow. Represented in the password reset process progress bar.

- Type: integer
- Default value: 90000 (milliseconds)
- Location: Password Reset > Properties

**password_reset.wf.timeout**

Specifies the maximum wait time, in milliseconds, for the workflow to execute. The workflow is triggered during the password reset request when the user clicks **Submit**.

- Type: integer
- Default value: 500 (milliseconds)
- Location: Password Reset > Properties

**promin.show_records.limit**

Specifies the maximum number of records that can be returned for an arc or node for the **Show Records** link to display. If more records are returned than the set limit, the link does not display.

- Type: integer
- Default value: 100,000 (records)
- Location: Add the property to the System Property [sys_properties] table.

**remember_me.max_duration_in_days**

Sets a maximum cap for the **remember_me_cookie.duration_in_days** cookie to expire before forcing a user to reauthenticate into the instance.

- Type: integer
- Default value: 30 (days)

Note: Maximum value 365 days.
• Location: System Property [sys_properties] table

**remember_me_cookie.duration_in_days**
Sets the default expiration for the "remember me" cookie. When a user logs in with "remember me" enabled, each login within the expiration limit resets the expiration period.

- Type: integer
- Default value: 15 (days)

**Note:** Maximum value 30 days.

• Location: System Property [sys_properties] table

**sa_analytics.aggregation.include_service**
Includes all CIs for alert aggregation. If **false**, includes only CIs not related to a business service.

- Type: true | false
- Default value: true
- Location: Alert Aggregation and RCA > Properties

**sa_analytics.aggregation_enabled**
Enables alert aggregation. Enables aggregation of correlated alerts for services and alert groups.

- Type: true | false
- Default value: true
- Location: Alert Aggregation and RCA > Properties

**sa_analytics.alert.severity_threshold**
Alert severity threshold, above which alerts are included in analysis. Only alerts with severity that is above the threshold are included in alert aggregations and root cause CI analysis.

- Type: choice list
- Default value: Info
- Other possible values:
  - Warning
  - Minor
  - Major
  - Critical
- Location: Alert Aggregation and RCA > Properties

**sa_analytics.rca_enabled**
Enables (**true**) or disables (**false**) root cause analysis for business services. Enables RCA for alerts associated with business services, to identify root-cause CIs.

- Type: true | false
- Default value: false
- Location: Alert Aggregation and RCA > Properties

**sa_analytics.rca.input_purge_days**
Purge staging tables (in days). Number of days that RCA input is kept before it is purged.
• Type: integer
• Default value: 90
• Range of possible values: 30-180
• Location: Alert Aggregation and RCA > Properties

`sa_analytics.rca.learner_group_interval_secs`
Time interval (in seconds) criteria for grouping alerts. Interval that alerts must be created in, to be included in a group.
• Type: integer
• Default value: 300
• Range of possible values: 60-900
• Location: Alert Aggregation and RCA > Properties

`sa_analytics.rca.learner_query_interval_secs`
Length of time period (in seconds) from which to include alerts for analysis. Period of past time from which to include alerts in alert aggregation analysis.
• Type: integer
• Default value: 86400
• Range of possible values: 43200-86400
• Location: Alert Aggregation and RCA > Properties

`sa_analytics.rca.output_purge_days`
Number of days that RCA output is kept before it is purged.
• Type: integer
• Default value: 3
• Range of possible values: 3-5
• Location: System Property [sys_properties] table

`sa_analytics.rca.query_probability_threshold`
Confidence score % threshold, above which RCA correlated alert groups appear in the Event Management dashboard and alerts console. Confidence score that must be met by RCA correlated alert groups before the groups are displayed on the Event Management dashboard and alerts console.
• Type: integer
• Default value: 0
• Range of possible values: 0-100
• Location: Alert Aggregation and RCA > Properties

`sam.install_deletion_deadline`
Defines the number of days after which a software install is deleted if not discovered with the configuration item. Use a value that is greater than the number of days between consecutive Discovery runs.
• Type: integer
• Default value: 7
• Location: System Property [sys_properties] table

`security.list.internal.domains`
Other domains (excluding the ones in the comma-separated list in this property) are classified as external email domains. The counts of incoming emails from these external domains display in the External Incoming Emails metric in the Instance Security Center.

- Type: choice string
- Default value: None
- Other possible values: Comma-separated list of all internal email domains in the organization.
- Location: System Property [sys_properties] table

**sn_bm_client.dashboard_display_unit**

Time unit to use for KPI values on the Benchmarks dashboard. Options are Hours or Days.

- Type: choice list
- Default value: Days
- Location: System Property [sys_properties] table

**sn_chg_soc.change_soc_initial_limit**

Defines the number of change_request records to display on load of the Change Schedule.

- Type: Integer
- Default value: 40
- Location: System Property [sys_properties] table

**sn_chg_soc.change_soc_scroll_load_limit**

Defines the number of change_request records to display as the Change Schedule is scrolled.

- Type: Integer
- Default value: 20
- Location: System Property [sys_properties] table

**sn_chg_soc.change_soc_total_limit**

Defines the total number of change_request records that can be displayed on a Change Schedule.

- Type: Integer
- Default value: 1000
- Location: System Property [sys_properties] table

**sn_chg_soc.landing_page.pinned_notification**

Shows a message for pin or unpin a change schedule.

- Type: true | false
- Default value: true
- Location: System Property [sys_properties] table

**sn_chg_soc.schedule_window_days**

Specifies the number of days to be factored before and after the respective start/end of a change_request record when displaying blackout and maintenance window spans on the Change Schedule page.

- Type: Integer
- Default value: 30
- Location: System Property [sys_properties] table
sn_disco_cd.scheduled_job_time_out_in_mins

This property sets the value for the maximum run time of the scheduled job for Cloud Resources in minutes.

- Type: integer
- Default value: 120

sn_global_searchui.hide_results_count

Hides (true) or displays (false) the number of matching records for search groups and tables on the Global Search page.

To modify this property, select Enhanced Global Search UI from the application picker before opening the System Properties table.

- Type: true | false
- Default value: false
- Location: System Property [sys_properties] table

subscription.custom_table.enforce_entitlement

You can enable guardrails around custom tables when using certain applications, such as Mobile Studio, in a production or non-production environment.

When set to true, the property limits the list of custom tables available in applications such as Mobile Studio to those you are entitled to use, based on the active subscriptions present on your instance. If you want to remove these guardrails, setting the property to false enables you access to all custom tables, regardless of your active subscription entitlements.

- Type: Boolean
- Default value:
- Location: System Property [sys_properties] table

Note: Setting this property to false enables you to use applications with custom tables that may not be entitled. See the service description for your active subscriptions to determine which custom tables (if any) you are entitled to use with selected applications.

tablet.footer.text

Text that appears on the footer of the tablet UI.

- Type: string
- Default value: Copyright ServiceNow 2012
- Location: System Properties > Tablet UI Properties

tablet.header.text

Text that appears on the right-hand side of the tablet UI header.

- Type: string
- Default value: ServiceNow
- Location: System Properties > Tablet UI Properties
Add a system property

Add or create a property to control system behavior.

Role required: admin

For more information on creating system properties for your own applications, take the training on the ServiceNow® Developer Site.

Some properties in the system are not visible in an instance by default and must be added to the System Property [sys_properties] table. If a feature requires the addition of the property, you can add a system property.

**Important:** System properties store configuration information that rarely or never changes. Each time you change or add a system property, the system flushes the cache to keep all nodes in the cluster in synch. This cache flush has a very high performance cost for one to ten minutes, which can potentially cause an outage if done excessively. To prevent such outages, do not use a system property to store configuration information that changes more than once or twice a month. Instead, use a custom table to store regularly changing configuration information.

1. In the Navigation filter, enter `sys_properties.list`. The entire list of properties in the System Properties [sys_properties] table appears.
2. Verify that the property does not exist by searching for the property name.
3. Click New.
4. Complete the System Property form using the database name of the property.

Make sure to specify the correct data **Type** and add the new value that you want the property to use.

Properties that you add already contain default values. You add properties to change this value.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the property you are creating.</td>
</tr>
<tr>
<td>Description</td>
<td>Type a brief, descriptive phrase describing the function of the property.</td>
</tr>
<tr>
<td>Choices</td>
<td>Comma-separated values for a choice list. If you need a different choice list label and value, use an equal sign (=) to separate the label from the value. For example, Blue=0000FF, Red=FF0000, Green=00FF00 displays Blue, Red, and Green in the list, and saves the corresponding hex value in the property value field.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the appropriate data type from the list (for example, integer, string, or true</td>
</tr>
<tr>
<td>Value</td>
<td>Set the desired value for property. All property values are stored as strings. When retrieving properties via the <code>gs.getProperty()</code> method, treat the results as strings. For example, a true</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Ignore cache</td>
<td>The system stores system property values in server-side caches to avoid querying the database for configuration settings. When you change a system property value, the system always flushes the cache for the sys_properties table. Use this field to determine whether to flush this property's value from all other server-side caches. The default value of false causes the system to not ignore flushing caches, which results in flushing all server-side caches and retrieving the current property value from the database. Set this field to false when you want to ensure all caches have the current property value. The true value causes the system to ignore flushing some server-side caches, which results in only flushing the cache for the sys_properties table and preserving the prior property value in all other caches. Set this field to true to avoid the performance cost of flushing all caches and retrieving new property values. Typically, you should only set this field to true when you have a system property that changes more frequently than once a month, and the property value is only stored in sys_properties table.</td>
</tr>
<tr>
<td>Private</td>
<td>Set this property to true to exclude this property from being imported via update sets. Keeping system properties private prevents settings in one instance from overwriting values in another instance. For example, you may not want a system property in a development instance to use the same value as a production instance.</td>
</tr>
<tr>
<td>Read roles</td>
<td>Define the roles that have read access to this property.</td>
</tr>
<tr>
<td>Write roles</td>
<td>Defines the roles that have write access to this property.</td>
</tr>
</tbody>
</table>

5. Click Submit.

Depending on the property name, an administrator might be able to change its value only through a new module. It may also appear in one of the Properties pages in System Properties.

Note: If the Ignore cache check box is selected, the system flushes the server cache when the parameter is changed.

Create a system properties module

You can add a module in the application navigator to access the list of system properties. This module makes it easy to add properties to the System Properties table.

Role required: admin

1. Navigate to System Definition > Application Menus.
2. Search for the application you want to add the properties table to, for example System Properties.
   Select an application that is restricted to the admin role so that non-admin users cannot access it.
3. From the Modules related list, click New.
4. Complete the form fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Module name. For example, <strong>All Properties</strong>.</td>
</tr>
<tr>
<td>Application Menu</td>
<td>Specifies the name of the application menu the module appears under. This field should automatically be populated with the name of the application you accessed the Modules related list from.</td>
</tr>
<tr>
<td>Link type</td>
<td>Specifies the type of link this module opens. For a list of system properties, select <strong>List of Records</strong>.</td>
</tr>
<tr>
<td>Table</td>
<td>Specifies the table used by the module. Select <strong>System Properties [sys_properties]</strong>.</td>
</tr>
</tbody>
</table>

5. Click **Submit**.

6. Verify that the module was created. For example, navigate to **System Properties > All Properties**.

If you want to include additional parameters for the list of system properties module, see [Create a module](#).

**Handle HTTP 500 errors**

The HTTP 500 error is a generic error message that Internet Explorer passes to you when your web site errors for one reason or another, but it provides no useful information by itself.

We can change this setting, to allow you to see and read what the real error is. Good error information is essential to the debugging of any application, and the HTTP 500 error may in fact provide more information to the Customer Service and Support team.
To enable Internet Explorer to show you the root cause of any error in your code, you need to make a change in the Internet Options window. You can access the Internet Options window by selecting the Internet Options item from the Tools menu at the top of Internet Explorer.

1. Select the Advanced tab.
2. Accessing the Advanced options displays a window that contains many settings that can be changed within Internet Explorer. These settings are broken down into categories. The category we are interested in is the **Browsing** Category.

3. Scrolling down the window will bring you to the **Show friendly HTTP error messages** check box. By default this box is checked in order to hide the real error from users. Once you have located this check box, remove the check and click the **OK** button.

You can now report any problem pages that you have had difficulty with and see the real error message that is being generated. Once you can see what the real error message is, then providing debugging information to the Customer Service and Support team becomes so much easier.
Query join and complexity size limits

The platform uses a relational database to store data. Retrieving data can involve multiple joins to create a single result set. While these joins are usually simple, in certain cases the system may issue very large joins to bring together large numbers (>20) of tables.

Database engines normally handle multiple joins quite well. The relational model assumes joins are cheap and efficient, and this is usually true. Rarely, however, exceedingly large joins may cause a database performance issue.

To mitigate this potential complexity, use the following property to limit join complexity and size.

Navigate to **System Properties > System** and find the property with this description:

**Max number of database joins per query. Smaller values cause the system to issue a larger number of less complex queries. Larger values reduce the number of queries at the cost of additional complexity per query. In the absence of known database issues stemming from large join counts, this property should remain unchanged.**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.http.proxy_host</td>
<td>Specify the proxy server hostname or IP address.</td>
<td>proxy.company.com, 192.168.34.54</td>
</tr>
</tbody>
</table>

Note: In the absence of known database issues stemming from large join counts, this parameter should remain unchanged.

Query complexity limits

This property specifies the maximum number of joins the system prefers to do. In certain edge cases, more complex queries might need to be issued, but generally no more than this number of joins will be issued. e.g., a value of 10 will result in no more than 10 tables being joined together in any given query.

The system must compensate for the fewer joins by issuing more queries to retrieve necessary data, so tuning this number down will result in more queries being sent to the database. In most cases, tuning this parameter is counterproductive.

Web proxy

Several properties support Web proxy configuration.

Note: Set these properties in the **System Properties** [sys_properties] table.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.http.proxy_host</td>
<td>Specify the proxy server hostname or IP address.</td>
<td>proxy.company.com, 192.168.34.54</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved. ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
### Property

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.http.proxy_port</td>
<td>Specify the port number for the proxy server.</td>
<td>8080, 9100</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Default value: none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Examples</td>
<td></td>
</tr>
<tr>
<td>glide.http.proxy_username</td>
<td>Specify the username used to authenticate the proxy server.</td>
<td>proxyuser</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Default value: none</td>
<td></td>
</tr>
<tr>
<td>glide.http.proxy_password</td>
<td>Specify the password used to authenticate the proxy server.</td>
<td>password</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Default value: none</td>
<td></td>
</tr>
<tr>
<td>glide.email.override.url</td>
<td>Set the URL to use in emailed links in place of the instance URL. The URL</td>
<td><a href="https://servicenow.customerdomain.com/production/nav_to.do">https://servicenow.customerdomain.com/production/nav_to.do</a></td>
</tr>
<tr>
<td></td>
<td>should end with nav_to.do.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Default value: instance URL</td>
<td></td>
</tr>
</tbody>
</table>

### NTLM authentication

NTLM is the most complex of the authentication protocols supported by a basic web server.

NTLM is the most complex of the authentication protocols supported by a basic web server such as HttpClient. It is a proprietary protocol designed by Microsoft with no publicly available specification. Early versions of NTLM were less secure than Digest authentication due to faults in the design. However, these were fixed in a service pack for Windows NT 4 and the protocol is now considered more secure than Digest authentication.

NTLM authentication requires that an instance of NTxCredentials be available for the domain name of the server or the default credentials. Since NTLM does not use the notion of realms, HttpClient uses the domain name of the server as the name of the realm. Also, the username provided to the NTxCredentials should not be prefixed with the domain:

- Correct: adrian
- Incorrect: DOMAIN\adrian

There are some significant differences in the way NTLM works compared with basic and digest authentication. These differences are generally handled by HttpClient. However, having an understanding of these differences can help you avoid problems when using NTLM authentication.

- NTLM authentication works almost exactly the same as any other form of authentication in terms of the HttpClient API. The only difference is that you need to supply NTxCredentials instead of UsernamePasswordCredentials (NTxCredentials actually extends UsernamePasswordCredentials so you can use NTxCredentials right throughout your application, if needed).
- The realm for NTLM authentication is the domain name of the computer being connected. This can be troublesome because servers often have multiple domain names. Only the domain name that HttpClient connects to, as specified by the HostConfiguration, is used to look up the credentials. While initially testing NTLM authentication, it is best to pass the realm in as null, which is used as the default.
- NTLM authenticates a connection and not a request. So you need to authenticate every time a new connection is made and keeping the connection open during authentication is vital. For this reason, NTLM cannot be used to authenticate with both a proxy server and the web server, nor can NTLM be used with HTTP 1.0 connections or web servers that do not support HTTP keep-alives.

**Note:** Set these properties from the System Properties `[sys_properties]` table.

### NTLM authentication

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.http.proxy_ntusername</td>
<td>Specify the username used to authenticate the proxy server with NTLM authentication.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
<td>username</td>
</tr>
<tr>
<td></td>
<td>• Default value: none</td>
<td></td>
</tr>
<tr>
<td>glide.http.proxy_ntpassword</td>
<td>Specify the password used to authenticate the proxy server with NTLM authentication.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
<td>password</td>
</tr>
<tr>
<td></td>
<td>• Default value: none</td>
<td></td>
</tr>
<tr>
<td>glide.http.proxy_nthost</td>
<td>Specify the hostname used to authenticate the proxy server with NTLM authentication.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
<td>nthost</td>
</tr>
<tr>
<td></td>
<td>• Default value: none</td>
<td></td>
</tr>
<tr>
<td>glide.http.proxy_ntdomain</td>
<td>Specify the domain used to authenticate the proxy server with NTLM authentication.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
<td>DOMAIN</td>
</tr>
<tr>
<td></td>
<td>• Default value: none</td>
<td></td>
</tr>
</tbody>
</table>

### Proxy servers for SOAP clients

Administrators can specify separate proxy settings for SOAP clients, such as the MID Server or ODBC Driver.

To specify a proxy server for a MID Server, see [MID Server configuration](#).

To specify a proxy server for the ODBC driver, see [Configure ODBC to use proxy servers](#).

### Bypass the proxy server

Administrators can configure the instance to bypass the proxy server for specific URLs or URL patterns.

Typically, internal addresses do not need a proxy server for SOAP communications.
**Table administration**

A table is a collection of records in the database. Each record corresponds to a row in a table, and each field on a record corresponds to a column on that table.

Applications use tables and records to manage data and processes, such as Incident, Problem, and CMDB. Tables can extend other tables, creating parent tables and child tables.

Watch this nine-minute video for an introduction to tables, records, and fields in ServiceNow®.

Administrators can use these tools for viewing and modifying the database structure:

- Tables module: Provides a list of all tables in the database.
- Tables & Columns module: Provides a list of all existing tables, with columns, column attributes, and indexes.
- Schema map: Provides a graphical representation of the relationships between tables.
- Data dictionary tables: Contains additional information that defines database elements.

**Table extension and classes**

Enable one or more child tables to share fields and records with a parent table. Administrators and application developers can only extend tables during table creation.

Administrators and application developers typically extend tables to create a set of related records that share information. For example, in the base system, the Task and the Configuration Item tables have multiple extensions:

**Sample extended tables in the base system**

<table>
<thead>
<tr>
<th>Original table</th>
<th>Related tables extended from original table</th>
</tr>
</thead>
</table>
| Task [task]           | • Incident [incident]  
|                       | • Problem [problem]  
|                       | • Change Request [change_request]                                  |
| Configuration Item [cmdb_ci] | • Application [cmdb_ci_appl]  
|                       | • Computer [cmdb_ci_computer]  
|                       | • Database [cmdb_ci_database]                                      |
A table that extends another table is called a child class, and the table it extends is the parent class. A table can be both a parent and child class both extending and providing extensions for other tables. A parent class that is not an extension of another table is called a base class.

Administrators can use these tools to see the relationships between classes.

- Schema map
- System dictionary
- Tables module

Extending a table:

- Links the new table to the extending table.
- Creates system fields in the new table.
- Creates one or more database tables to store the parent and child classes. The number of tables the system creates depends upon the extension model selected during table creation.

Extension models

The Now Platform offers these extension models.

- Table per class
- Table per hierarchy
- Table per partition

The extension model determines these attributes.

- The number of database tables created
- The derivation of fields from parent classes
- The replication of records from child classes

Table per class

Tables created
Creates a separate database table for the parent class and each child class.

Fields derived from parent class
Child classes derive fields from parent classes.

Dictionary records created for parent class
A parent class has a Dictionary record for the collection and for each field that can be derived from it. For example, the Contract [ast_contract] table has 59 Dictionary records, which define the table and its fields.

Dictionary records created for child classes
Each child class only has Dictionary entries for fields unique to the class.

Records replicated
The parent class replicates each record stored in its child classes. Each child class only stores records unique to the class. Replicated records have the same Sys ID value in each table. The system replicates any change you make to a child record to the matching record in the parent table. For example, Contract [ast_contract] table replicates records from the Lease [ast_lease] and Warranty [ast_warranty] tables.
Table per hierarchy

Tables created
Creates one database table for the parent class, which stores all records for the parent and child classes. Child classes do not have separate database tables.

Fields derived from parent class
Child classes derive fields from parent classes. For example, the Incident table derives fields from the Task table.

Dictionary records created for parent class
A parent class has a Dictionary record for the collection and for each field that can be derived from it. For example, the Task table is a parent class that has 66 Dictionary records, which define the table and its fields.

The Dictionary entry for the parent class contains a sys_class_name column whose value indicates which child class each record belongs to. For example, Incident records have a sys_class_name value of incident, and change records have a sys_class_name value of change.

Dictionary records created for child classes
Each child class only has Dictionary entries for fields unique to the class. For example, the Incident table only has 22 Dictionary records, which are not already defined in the Task table.

Records replicated
Record replication is not needed, because the parent class stores all records that belong to the hierarchy. For example, the Task table contains all records from its child classes such as the Change, Incident, and Problem tables.

Table per partition

Tables created
Creates one database table for the parent class, which stores all records for the parent and child classes. Child classes do not have separate database tables. As the database table reaches a storage limit, the system dynamically adds storage tables (partitions) to store additional records.

Fields derived from parent class
Child classes do not derive fields from parent classes. Instead each child class has its own list of fields. For example, the Base Configuration Item [cmdb], Configuration Item [cmdb_ci], and Hardware [cmdb_ci_hardware] tables all have their own field definitions.

Dictionary records created for parent class
A parent class has a Dictionary record for the collection and for each field relevant to it. For example, the Base Configuration Item [cmdb] table is a parent class that has 48 Dictionary records.

The system replicates changes made to parent class Dictionary entries to child class Dictionary entries. For example, when you change the name column in the parent class Base Configuration Item [cmdb] table, the system replicates it to child class Dictionary entries such as the Configuration Item [cmdb_ci] and Hardware [cmdb_ci_hardware] tables.

The Dictionary entry for the parent class contains columns for sys_class_name and sys_class_path whose values indicate which child class each record belongs to. For example, Hardware records have a sys_class_name value of cmdb_ci_hardware, and computer records have a sys_class_name value of cmdb_ci_computer.

When the database table reaches a storage limit, the system updates the Dictionary entry for the parent class to include columns for sys_storage_alias and storage_table_name. These storage column Dictionary entries allow administrators to manage the parent class and its storage tables as a single logical unit.
Dictionary records created for child classes

Each child class has a Dictionary record for the collection and for each field relevant to it. For example, the Hardware table has 73 Dictionary records with some records duplicating columns in the parent class.

Records replicated

Record replication is not needed, because the parent class stores all records that belong to the hierarchy. For example, the Base Configuration Item [cmdb] table contains all records from its child classes such as the Application [cmdb_ci_appl], Computer [cmdb_ci_computer], and Hardware [cmdb_ci_hardware] tables.

Create a table

Administrators and application developers can create custom tables to store application data.

Role required: admin

Now Platform application subscriptions include custom table entitlements. You can create custom tables for any purpose, up to the entitlement limit in the subscription. To learn more about how your usage administrator allocates the custom tables that you create to subscriptions, see Allocating your custom tables to a subscription entitlement.

Note: To minimize the existence of unneeded and extraneous tables in an instance, don't overdo table creation. Create only those tables you need to minimize administration tasks and shorten upgrade times.

1. Navigate to System Definition > Tables.
2. Click New and complete the form.

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>Enter a unique label for the table (such as Laptops or Thin Clients). The label appears on list and form views for the table. Updating the Label field also updates the label record in the language file for the current language. See Field Labels in Data dictionary tables.</td>
</tr>
</tbody>
</table>
| Name    | Edit the table name, which is automatically populated based on the table label and a prefix as follows:  
• For a table in a scoped application, the name is prefixed with a namespace identifier to indicate that it is part of an application.  
• For a table in the global application, the name is prefixed with the string u_.  
• For a remote table in a scoped application, the name is prefixed with a namespace identifier and the string st__ to indicate that it is remote and part of an application.  
• For a remote table in the global application, the name is prefixed with the string u_st__.  
You cannot modify the prefix; however, you can modify the rest of the table name. The name can contain only lowercase, alphanumeric ASCII characters and underscores (_). |
### Control

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extends Table</td>
</tr>
<tr>
<td>Application</td>
</tr>
<tr>
<td>Remote Table</td>
</tr>
<tr>
<td>Create module</td>
</tr>
<tr>
<td>Add module to menu</td>
</tr>
</tbody>
</table>

### Column

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Column label</td>
</tr>
</tbody>
</table>

3. In the **Columns** section, use the **Table Columns** embedded list to add columns to the table.
<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>[Mandatory] Define the field type for the column. See <em>Introduction to Fields</em> and <em>Field types</em>. To preserve existing data, only change fields between the same basic type (for example, <em>Choice</em> and <em>String</em>). A warning appears if a change to a custom field results in data loss. You cannot change a base system field, that results in data loss.</td>
</tr>
</tbody>
</table>
| **Reference** | Make the field into a reference field by entering the referenced table name.  

**Note:** Dynamic reference creation is enabled for this field. So, if you enter a table name that does not match an existing table, a new table is created when you save changes to the current table record. If the current table has a module in the application navigator, then a module for the newly created table is automatically created in the same application menu. |
| **Max length** | [String fields only] Limit the length of the field. A length of under 254 appears as a single-line text field. Anything 255 characters or over appears as a multi-line text box.  

**Note:**  
- You can only change this value if the *Type* of the field is *String*. Changes for any other type of field are ignored.  
- On an Oracle instance, you cannot increase the maximum length of a string field to greater than 4000 because it requires the CLOB datatype in Oracle. To increase beyond this size, log an incident with ServiceNow Technical Support to request the change.  
- To prevent data from being lost, only decrease the length of a string field when you are developing a new application and not when a field contains data. A warning appears if a change to a custom field results in data loss. For a base system field, you cannot make a change that results in data loss. |
| **Default value** | Specify the default value of the field for any new record. Ensure that this value uses the correct field type. For example, an integer field can use a default value of 2 but cannot use a default value of *two*. These values can be overridden with dictionary overrides. |
4. In the **Controls** section, define additional table options.

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extensible</td>
<td>Select the check box to enable other tables to extend this table. Clear the check box to prevent the creation of additional child tables; existing child tables remain unchanged.</td>
</tr>
<tr>
<td>Live feed</td>
<td>Select the check box to enable record feeds for the table. This option adds the <strong>Show Live Feed</strong> icon in the form header.</td>
</tr>
<tr>
<td>Auto-number</td>
<td>Select the check box, and then define the number format to add an auto-numbered field to the table. The check box is available only when a number format does not exist for the table. Otherwise, you can edit the existing number format.</td>
</tr>
<tr>
<td>Create access controls</td>
<td>Select the check box and then complete the <strong>User role</strong> field to create basic security rules for the table.</td>
</tr>
<tr>
<td>User role</td>
<td>Enter a new name or select an existing user role that is required to access this table. This option is available only when the <strong>Create access controls</strong> check box is selected.</td>
</tr>
</tbody>
</table>

5. In the **Application Access** section, define the scope protection for the table. For more information, see Application access settings.

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accessible from</td>
<td>Specify which application scopes can access the table:</td>
</tr>
<tr>
<td></td>
<td><strong>All application scopes</strong> Can be accessed from any application scope.</td>
</tr>
<tr>
<td></td>
<td><strong>This application scope only</strong> Can be accessed only from the current application scope.</td>
</tr>
<tr>
<td>Can read</td>
<td>Select the check box to enable script objects from other application scopes to read records stored in this table. This option offers runtime protection. For example, a script in another application can query data on this table. First select read access to grant any other API record operation.</td>
</tr>
<tr>
<td>Control</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Can create</td>
<td>Select the check box to enable script objects from other application scopes to create records in this table. This option offers runtime protection. For example, a script in another application can insert a new record in this table. This option is available only when the Can read check box is selected. Clear the check box to prevent script objects from other application scopes from creating records in this table.</td>
</tr>
<tr>
<td>Can update</td>
<td>Select the check box to enable script objects from other application scopes to modify records stored in this table. This option offers runtime protection. For example, a script in another application can modify a field value on this table. This option is available only when the Can read check box is selected. Clear the check box to prevent script objects from other application scopes from modifying data stored in this table.</td>
</tr>
<tr>
<td>Can delete</td>
<td>Select the check box to enable script objects from other application scopes to delete records from this table. This option offers runtime protection. For example, a script in another application can remove a record from this table. This option is available only when the Can read check box is selected. Clear the check box to prevent script objects from other application scopes from deleting records from this table.</td>
</tr>
<tr>
<td>Allow access to this table via web services</td>
<td>Select the check box to enable users to make inbound Web services web service queries to this table. This option offers both design-time and runtime protection. The user performing the query must have the correct permissions to access this table, even when this check box is selected. Clear the check box to prevent users from making web service queries to this table.</td>
</tr>
<tr>
<td>Allow configuration</td>
<td>Select the check box to enable applications from other application scopes to create configuration records for this table that change its functionality. For example, an application designer can select this table from the Tables list on business rules, client scripts, or UI actions. This option offers design-time protection. Clear the check box to prevent application designers from selecting this table when creating configuration records.</td>
</tr>
</tbody>
</table>

6. Click **Submit**.
Global default fields

When you create a new custom table, several fields appear in the **Table Columns** embedded list. For all tables, required system fields are added automatically. You cannot delete or modify these fields.

For tables that extend another table, fields on the parent table also appear on the **Table Columns** embedded list for the current table. If you modify these fields, remember that all changes to fields on the parent table also affect all child tables, not just the current table.

These required system fields are added to all tables:

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class [sys_class_name]</td>
<td>System Class Name</td>
<td>If the table is extensible, a string field that indicates which child table contains the record.</td>
</tr>
<tr>
<td>Created [sys_created_on]</td>
<td>Date/Time</td>
<td>A time-stamp field that indicates when a record was created.</td>
</tr>
<tr>
<td>Created by [sys_created_by]</td>
<td>String</td>
<td>A string field that indicates the user who created the record.</td>
</tr>
<tr>
<td>Sys_id [sys_id]</td>
<td>Sys ID</td>
<td>The unique record identifier for the record.</td>
</tr>
<tr>
<td>Updates [sys_mod_count]</td>
<td>Integer</td>
<td>A numeric field that counts the number of updates for this record since record creation.</td>
</tr>
<tr>
<td>Updated by [sys_updated_by]</td>
<td>String</td>
<td>A string field that indicates the user who most recently updated the record.</td>
</tr>
<tr>
<td>Updated [sys_updated_on]</td>
<td>Date/Time</td>
<td>A time-stamp field that indicates the date and time of the most recent update.</td>
</tr>
</tbody>
</table>

Tables module

The Tables [sys_db_object] table contains a record for each table in the database.

To view the list of tables, navigate to **System Definition > Tables**. For example, you can filter the list to see extended table relationships.
Extended Table Relationships

To open the record for an existing table, click a table label. You can:

- View, add, or modify columns with a searchable and sortable embedded list, define the auto-number format, make the table extendable by other tables, and create modules for the table.
- Launch a schema map for a table by clicking the Show Schema Map related link.
- Open the dictionary entries for the table by right-clicking the form header and selecting Show Dictionary Record.
- Navigate directly to the default list or form view for the table by clicking the Show List or Show Form related link.
- Delete all records from a table by clicking the Delete All Records.
Delete a table

Administrators can delete custom tables that are no longer needed. For example, delete a table from an application that is under development because the business requirements change.

A table is custom if an administrator created it and it is not part of a system upgrade or plugin activation. Custom table names always begin with `u_` or `x_` for scoped tables.

⚠️ **Warning:** You cannot delete base system tables. If you inadvertently delete such a table, it is automatically recreated when you upgrade an instance.

You cannot delete a table that has associated tables that extend from it.
You must first delete all records in the table before you delete the table itself. If you do not first delete the records, errors can result on the parent table if it references the records. Deleting the records removes any references from the parent table. To learn more, see delete the records in the table.

Delete a custom table

If you no longer need a custom table, you can delete it after you delete all the records in the table.

1. Navigate to System Definition > Tables.
2. Open the table to delete.
3. Click Delete All Records.

   Deleting all records before deleting the table ensures that the business logic is properly executed (for example, reference cascade rules or other delete business rules). If you do not delete all records from the table first, then you must manually fix any other records or tables that the table deletion impacts.

4. Click Delete.
5. In the confirmation dialog box, enter delete and click OK.

   The table and all items that reference the table are deleted, including:
   - Choice list items
   - Forms, form sections, lists, and related lists
   - Reports and Performance Analytics widgets
   - Reference fields that reference the table
   - Access controls

Delete all records from a table

You may decide to delete all the records on a table without deleting the table itself. For example, the administrator may want to delete all incidents on a test instance without deleting the incident table itself.

When you prepare to delete many records from a table, consider the following guidelines to minimize impact on performance.

- Limit the number of records to be deleted in a single delete action to prevent the table from being locked. Use the `setLimit()` method described at `setLimit`.
- Minimize triggering an excessive number of business rules as a result of this deletion. Use the `setWorkflow(Boolean e)` method described at `setWorkflow`.

**Note:** Deleting all records for a table also deletes records from tables that extend the table.

There are several methods for deleting table records. Depending on the number of records to be deleted, choose the method that would be most efficient in your environment. Use these methods with caution. Before performing this procedure, be sure that you do not need any of the records.
• From the **Tables and Columns** module, complete the following steps.
  a) Navigate to **System Definition > Tables and Columns**.
  b) Select the table for which to delete records.

  ![Table and Columns](image)

  **Tables & Columns**
  Click a button to create a new table or application, or browse all applications.

  ![Create Table](image)  ![Create Application](image)  ![Browse Applications](image)
c) Click **Delete all records**.

d) In the confirmation dialog box, enter `delete` and click **OK**.

- From a list view, complete the following steps.
  a) In List v2, navigate to the list view that displays the table records, click the context menu, and then navigate to **Show**.
  b) In List v3, click **<Number> rows per page** in the footer.
  c) Set the number of rows per page to display the max number.
  d) Select all the rows on the page.
  e) Click **Actions on selected rows**, and then click **Delete**.
  f) Continue deleting all rows on a page until all records are deleted.

The selected table is empty of records. The table still exists, and any references to the table on other tables (such as business rules or reference fields) are preserved.

### Roll back and delete recovery

Recover deleted records and roll back some actions.

Recover individual records and all related changes, and roll back certain actions such as a patch upgrade, a plugin activation, and background script executions. The recovery and roll backs both use rollback contexts.

The roll back and delete recovery features are available on instances that use MySQL and MariaDB databases. Instances that use Oracle databases only support roll back. Instances that use SQLServer do not support roll back or delete recovery.

#### Roll back and delete recovery database support

<table>
<thead>
<tr>
<th>Database type</th>
<th>Roll back</th>
<th>Delete recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>MySQL</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>MariaDB</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Oracle</td>
<td>yes</td>
<td>no</td>
</tr>
</tbody>
</table>

### Deleted Records module

This module works on records in audited tables. Recovery of cascaded deleted records must be done within seven days of the record deletion. After seven days, only data records and references on tables that audit deletions can be recovered, which is the same functionality as prior releases.

To find this module, navigate to **System Definition > Deleted Records**.
Delete Recovery module

This module works for any deleted record. This recovery must be done within seven days of the record deletion.

To find this module, navigate to Rollback & Recovery > Delete Recovery.

Script Execution History module

This module works on scripts executed using the Scripts - Background module. This history only includes seven days of script executions.

To find this module, navigate to Rollback & Recovery > Script Execution History.

Rollback Contexts module

A rollback context is created for each patch upgrade within a family, and each plugin activation providing the plugin supports rollback contexts.

Note: Do not roll back a rollback context until checking with Customer Service and Support. A roll back deletes data and may remove evidence of the upgrade or activation issue preventing debugging of the problem.

The roll back must be done within seven days of the patch upgrade or plugin activation.

To find this module, navigate to Rollback & Recovery > Rollback Contexts.

Rollback contexts

Rollback contexts contain everything necessary to roll back a software upgrade or plugin activation. They include deleted records, patch updates, Scripts-Background script executions, database actions, and plugin activations.

Rollbacks are typically performed on pre-production instances where functionality must be restored before you can find the root cause of a problem in the upgrade. Rolling back deletes data, which can often make it hard if not impossible to discover the problem that made the rollback necessary.

A rollback context is created when:

• GlideRecord.delete() or GlideRecord.deleteMultiple() delete records.
• There is a patch upgrade.
• You activate a plugin that supports rollback contexts.
• A script executes using the Scripts-Background module, and rollback was enabled by selecting the Record for Rollback? check box.

Rollbacks do not impact other database activities. If a database activity modifies a record that is part of a rollback context, the rollback does not affect that record.

Because rollback contexts contain a significant amount of data, rollback contexts are deleted after seven days. Therefore, rollbacks must occur within seven days of the latest upgrade. Use the sys_property, glide.rollback.expiration_days to configure the number of days.

To use rollback contexts, activate the Restore Deleted Records and Delete Recovery plugins.

Rollback context excluded operations

If any of the following operations occur during a rollback, a rollback context is not created:
• Tables or columns are dropped from the schema.
  
  Index drops are okay.
• Table is truncated.
• Table or column is renamed.
• Column is reparented or promoted.
• Column type changes.
• Column width is decreased.

What happens on HI?

• The rollback process on HI updates the reported WAR to the rolled-back version.
• The assigned WAR remains set to the version before the rollback.
• `glide.war.no_upgrade` system property on the instance is set to the version before the rollback.
• The message, "Desired war matches reverted war specified by property [glide.war.no_upgrade]. Upgrade script will NOT run," appears during the rollback.
• Rollback context state says, "Expired."
• Rollback purges all stored data.

Roll back patch upgrades or plugin activations

Use the Rollback Contexts module to roll back patch upgrades and plugin activations.

• Rolling back is possible only between patches in the same software release.
  
  Rolling back is possible from London patch 2 to patch 1, but not from London to Kingston.
• Instances must be using Helsinki or later.
• Check with Customer Service and Support before rolling back pre-London instances.
• The rollback must be done within seven days of the most recent upgrade.

  Use the `glide.rollback.expiration_days sys_property` to configure the number of days. The default is seven.
• You can only roll back to the previous version.
  
  For example, rolling back from patch 3 to patch 1 requires two rollbacks.
• Rollback only supports MySQL.
• Restore Deleted Records and Delete Recovery plugins must be activated.
• You can only roll back one active instance at a time.
  
  Rolling back contexts on multiple nodes is not supported.
• A rollback deletes data and may remove evidence of an upgrade or activation record, which makes it difficult to debug the problem that made the rollback necessary.
• To roll back to a patch version before the Assigned WAR, submit a request for Customer Service and Support to do the rollback.

Role required: maint

2. Under **Related Links**, click **Rollback**.

![Rollback screenshot]

3. Confirm the rollback.
   
   An indicator appears showing the progress of the rollback. glide.war updates to the rolled-back version. App node stats.do updates shortly after the rollback completes. The log shows the stages of the rollback process.

4. After the rollback, restart the instance.
   
   Open a new tab and see if the context state changed to Rolled back.

### Use the Deleted Records module to restore a deleted record

You can recover deleted records that are in audited tables.

Role required: admin

The instance can track deletions on any table, and references on audited tables, with a few exceptions. Record deletions are not tracked in these circumstances.

- Record deletions are not tracked on tables with the **no_audit_delete=true** dictionary attribute.
- Deletions from tables with a sys prefix are not audited by default. You can configure specific system tables to audit deletions.
- References are restored only if the reference field is on an audited table and the Restore Deleted Record plugin is activated.


- References that use an Image field type are not restored.

1. Navigate to System Definition > Deleted Records.
2. Open the deleted record that you want to restore.

Note: You can only restore one deleted record and its associated references at a time.

3. Do one of the following to restore the record.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Undelete With Related</td>
<td>Recovers the record and all cascaded deletes and other database actions that resulted from the delete. This option appears when a rollback context is available for the delete.</td>
</tr>
<tr>
<td>Recover entire operation</td>
<td>If this record was deleted as part of another delete, all records from the parent delete are recovered including all cascaded deletes and other database actions that resulted from the parent delete. If this is the top level delete, then this is the same as Undelete with Related. This option appears when a rollback context is available for the delete.</td>
</tr>
<tr>
<td>Undelete Record</td>
<td>Recovers only this record.</td>
</tr>
</tbody>
</table>

An instructions page appears, explaining the process and its limitations.

4. Click Restore deleted record.
A Progress page shows the progress of the restore process, and shows a count of the references restored.

When the process completes, a Restore Summary itemizes the changes and provides links for viewing the restored record or returning to the deleted records list.

Use the Delete Recovery module to restore a deleted record

You can recover a deleted record and all related changes. The recovery must be done within seven days of the record being deleted.

Role required: admin

2. Click the item from the Delete Recoveries list to be recovered.
   The Delete Recovery form is shown.
3. Under Related Links, click Rollback....
4. In the Rollback entire operation form, enter yes, and click OK.
   A Progress page shows the progress of the restore process, and shows a count of the references restored.

When the process completes, a Restore Summary itemizes the changes and provides links for viewing the restored record or returning to the Delete Recoveries list.

Use the Script Execution History module to roll back a Scripts-Background execution

You can roll back the database actions of a script executed using the Scripts-Background module.

Role required: admin
When you executed the script using the Scripts-Background module, the Record for Rollback? item must have been checked.

If you are still in the Scripts-Background module after executing a script, you can use the Script execution history and recovery available here link to get to the Script Execution History form.

1. Navigate to Rollback & Recovery > Script Execution History.
2. Click the script execution to be rolled back.
3. In the Related Links, click Rollback Script Execution.

Create a table index

Constructing an effective index requires specialized knowledge in database architecture. If you do not have this expertise, you should consult someone who does.

Role required: admin

1. Navigate to System Definition > Tables & Columns.
2. In the list, find the table you want and click its label.
3. Navigate to the Database Indexes related list.
4. Click New.
5. Use the slushbucket to select the fields you want included in the index.
   The order in which you select the fields affects how the index works. If you do not have expertise in database design, you should consult someone who does.
6. To create a unique index, select the Unique Index check box.
7. Click Create Index.
   The Table Name field is there for your reference only. Overriding the default has no effect.

Task table

Task [task] is one of the core tables provided with the base system.

It provides a series of standard fields used on each of the tables that extend it, such as the Incident [incident] and Problem [problem] tables. In addition, any table which extends task can take advantage of task-specific functionality for driving tasks.

The Planned Task plugin provides the Planned Task [planned_task] table, which extends the Task [task] Table to provide more fields for tasks to measure duration and effort.

Create a task

Tasks are not created directly on the task table. Instead, tasks are created on task child tables.

1. Click the New button on the task record list, which launches the Task Interceptor.
2. Follow the on-screen instructions to locate the desired table that extends Task.

Define assignment rules

The instance can automatically assign a task to a user or group based on pre-defined conditions by using data lookup rules and assignment rules.
Assignment lookup rules example

In this example, the Data Lookup Plugin assignment lookup rule automatically assigns any incident with the Category of Request and Subcategory of Password Reset to Fred Luddy.

Assignment data lookup

Assignment rules module

The Assignment rules module allows you to automatically set a value in the assigned_to and assignment_group fields when a set of conditions occurs.

An assignment rule must also meet these additional criteria to run:

- The task record has been created or updated. Assignment rules do not apply to unsaved changes on a form.
- The task record must be unassigned. The record cannot have an existing value for either the assigned_to or assignment_group fields. Assignment rules cannot overwrite existing assignments (including assignments set by a default value or a previously run assignment rule).
- The assignment rule is the first rule that matches the table and conditions. If more than one assignment rule matches the conditions, only the rule with the lowest order value runs.

Condition editor example

In this example, the assignment rule uses a condition statement to automatically assign any incident opened in the Network category to the system administrator in the Network assignment group.

Assignment
Data lookup rules

Data lookup rules offer a generic way to change any field value, not just assignment fields.

Data lookup rules offer the following improvements over the Assignment module:

• Ability to change any field value not just an assignment field
• More options to define when a rule runs:
  • On form change (Allows assignment rules to apply to unsaved changes on a form)
  • On record insert
  • On record update
• Option to replace existing values (including default values)

Note: You can define data lookup and Assignment rules at the same time. The system ignores any duplicate rules after an incident has been assigned unless you are using a data lookup definition option to replace existing values.

Precedence between data lookup, assignment, and business rules

When creating new assignment rules, keep in mind that business rules can take precedence over assignment rules when they run after the assignment rule. Data lookup rules take precedence over assignment rules because they always run after.

Data lookup rules, assignment rules and business rules run in the following order:

1. All 'before' business rules that run on a record insert with an order value less than 1000.
2. All 'before' engines run, including assignment rules.
3. All 'after' engines run, including data lookup rules.
4. All 'before' business rules that run on a record insert with an order value greater than or equal to 1000.
5. All 'after' business rules that run on record insert.

Workflow assignments

An alternative to creating data lookup or assignment rules is to create one or more workflow tasks that assign a task record as part of a workflow.

Consider using a workflow for assignment if your process includes multiple steps or conditions such as requiring a particular group approve a request.

When using a workflow to manage task assignments, add a brief timer activity to the start of the workflow. Without this timer activity, the workflow runs before the parent record, the current record, is inserted into the database. After the timer activity completes, the workflow resumes using the parent record information from the database instead of the original current. Pausing a workflow in this way does not change a default workflow to a deferred workflow. For more information on how the workflow engine interacts with the database, see workflow engine operation order.
Baseline assignment rules example

A baseline instance contains certain assignment rules.

Baseline instance rules

<table>
<thead>
<tr>
<th>Name</th>
<th>Table</th>
<th>Conditions</th>
<th>Assigned to user, Assigned to group, or Script</th>
</tr>
</thead>
<tbody>
<tr>
<td>Networking</td>
<td>incident</td>
<td>Category is Network</td>
<td>User: System Administrator</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Group: Network</td>
</tr>
<tr>
<td>Database or Software</td>
<td>incident</td>
<td>Category is one of Request, Inquiry / Help, Software, Hardware</td>
<td>User: System Administrator</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Group: Software</td>
</tr>
<tr>
<td>SC Item fulfillment - Field Services</td>
<td>Ticket</td>
<td>Parent.Task.type is Request item</td>
<td>Group: Field Services</td>
</tr>
<tr>
<td>Release Planning</td>
<td>release_phase</td>
<td>Name is Plan</td>
<td>Script: current.release.product.service.assigned_to;</td>
</tr>
<tr>
<td>IT Hardware</td>
<td>sc_req_item</td>
<td>Approval is Approved and</td>
<td>User: System Administrator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Item.Category is Request Computers and Hardware</td>
<td>Group: Hardware</td>
</tr>
<tr>
<td>Service Desk</td>
<td>incident</td>
<td>Active is true</td>
<td>Group: Service Desk</td>
</tr>
</tbody>
</table>

Create an assignment rule

Create an assignment rule and apply it to a single table. Assignment rules are designed to run at the time you open a record.

Role required: assignment_rule_admin or admin
Example assignment rule

**Note:** An administrator can configure the form to see all the fields.

1. Navigate to **System Policy > Rules > Assignment** and click **New**.
2. Complete the form.

### Assignment rule form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The descriptive name for the assignment rule.</td>
</tr>
<tr>
<td>Active</td>
<td>Specifies whether the assignment rule is active. Only active assignment rules take effect.</td>
</tr>
<tr>
<td>Applies to</td>
<td>The table with the records that the assignment rule applies to.</td>
</tr>
<tr>
<td>Table</td>
<td>The list shows only tables and database views that are in the same scope as the assignment rule. If you select a custom table that extends the task table, and for the assignment rule to work properly, you must clear the instance cache by navigating to https://&lt;instance_name&gt;.service-now.com/cache.do.</td>
</tr>
</tbody>
</table>

**Note:** Clearing the system cache can affect overall performance, and degrade system response times. Do not run cache flushes during business hours, and do not trigger cache flushes automatically.

<table>
<thead>
<tr>
<th>Conditions</th>
<th>The conditions under which the assignment rule applies. In the example, the assignment rule applies when an incident is in the Network category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign to</td>
<td>The user the event is assigned to.</td>
</tr>
<tr>
<td>User</td>
<td>The group the event is assigned to.</td>
</tr>
<tr>
<td>Group</td>
<td></td>
</tr>
<tr>
<td>Script</td>
<td>A script to specify advanced assignment rule functionality. The current.variable_pool set of variables is available.</td>
</tr>
</tbody>
</table>

**Note:** Make sure the input in the script is correct, and that the input type matches the field type in the Assignment Rule script. For example, if the assignment rule script sets the value of an Integer field, and the value in the script is set to String, the assignment rule may yield unexpected results.

Other fields
Data lookup rules

You can define an assignment rule with Data Lookup and Record Matching Support.

2. Click New.
3. Populate the assignment data lookup fields (see table).
4. Click Submit.

Assignment data lookup fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Input value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Select the category the data lookup matches against.</td>
</tr>
<tr>
<td>Subcategory</td>
<td>Select the subcategory the data lookup matches against.</td>
</tr>
<tr>
<td>Configuration item</td>
<td>Select the configuration item the data lookup matches against.</td>
</tr>
<tr>
<td>Location</td>
<td>Select the location the data lookup matches against.</td>
</tr>
<tr>
<td>Assignment group</td>
<td>Select the assignment group to assign the incident to.</td>
</tr>
<tr>
<td>Field</td>
<td>Input value</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Assigned to</td>
<td>Select the user to assign the incident to.</td>
</tr>
<tr>
<td>Active</td>
<td>Set to Yes to run the rule or No to deactivate the rule.</td>
</tr>
<tr>
<td>Order</td>
<td>Enter the order in which the rule runs compared to other rules on the same table. The Data Lookup Plugin runs the rule with the lowest order and matching values.</td>
</tr>
</tbody>
</table>

**Note:** The assignment lookup rule assigns incidents matching the values in the matcher fields (Category, Subcategory, Configuration Item, and Location) to the values in the setter fields (Assignment Group and Assigned To). A valid assignment lookup rule requires at least one matcher field and one setter field.

**Important Task table fields**

The Task table is a base class that provides fields for the core ITSM applications such as Incident, Problem, and Change Management. All applications that extend the Task table share these fields in common.

<table>
<thead>
<tr>
<th>Label</th>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>active</td>
<td>boolean</td>
<td>Specifies whether work is still being done on a task or whether the work for the task is complete. By default, only application-specific business rules set the value of this field. For example, the incident autoclose business rule closes resolved incidents that have not been updated for one day.</td>
</tr>
<tr>
<td>Additional comments</td>
<td>comments</td>
<td>journal_input</td>
<td>Displays and allows the entry of comments about the task record. Each comment is inserted into the Activity field. For more information, see Journal Fields.</td>
</tr>
<tr>
<td>Approval History</td>
<td>approval_history</td>
<td>journal</td>
<td>Displays the history of approvals for the record. For more information, see Approvals.</td>
</tr>
<tr>
<td>Label</td>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Assigned To</td>
<td>assigned_to</td>
<td>reference</td>
<td>Specifies the user assigned to complete the task. By default, this field uses a reference qualifier to only display users with the itil role. Some applications override the parent reference qualifier to display relevant users. For example, the Service Order and Project Task tables filter users based on their skills.</td>
</tr>
<tr>
<td>Created</td>
<td>sys_created_on</td>
<td>glide_date_time</td>
<td>Displays the date and time when the task record was created.</td>
</tr>
<tr>
<td>Description</td>
<td>description</td>
<td>string</td>
<td>Displays and allows the entry of a multi-line description of the work to be done.</td>
</tr>
<tr>
<td>Escalation</td>
<td>escalation</td>
<td>integer</td>
<td>Indicates how long the task has been open. Escalations are dynamically populated using service level agreements, which specify how long a task remains in each escalation state. Escalation states go from Normal to Moderate to High, and finally to Overdue. Record lists color code each task by escalation state.</td>
</tr>
<tr>
<td>Number</td>
<td>number</td>
<td>string</td>
<td>Displays an identifying number for each task record. This field is the display value for the Task table. The system generates this number when the task is created. To manage number generation, see Number Maintenance.</td>
</tr>
<tr>
<td>Opened</td>
<td>opened_at</td>
<td>glide_date_time</td>
<td>Displays the date and time when a human opened the task record for the first time.</td>
</tr>
<tr>
<td>Label</td>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------</td>
<td>---------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Priority</td>
<td>priority</td>
<td>integer</td>
<td>Specifies how high a priority the task should be for the assignee. By default, the calculatePriority business rule calculates this value based on the Impact and Urgency values. Record lists color code each task by degree of priority.</td>
</tr>
<tr>
<td>Short Description</td>
<td>short_description</td>
<td>String</td>
<td>Displays and allows the entry of a short description of the task, which is a human-readable title for the record.</td>
</tr>
<tr>
<td>State</td>
<td>state</td>
<td>Integer</td>
<td>Displays a choice list for status of the task:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Pending</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Open</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Work in Progress</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Closed Complete</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Closed Incomplete</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Closed Skipped</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Applications typically use Dictionary overrides to display application-specific states.</td>
</tr>
<tr>
<td>Sys ID</td>
<td>sys_id</td>
<td>GUID</td>
<td>Displays the unique record identifier.</td>
</tr>
<tr>
<td>Task Type</td>
<td>sys_class_name</td>
<td>sys_class_name</td>
<td>Specifies the type of task, which corresponds to the child class. The system populates this value when a record is created on a child table.</td>
</tr>
<tr>
<td>Time Worked</td>
<td>time_worked</td>
<td>timer</td>
<td>Display a timer which measures how long a record is open in the form view.</td>
</tr>
<tr>
<td>Watch list</td>
<td>watch_list</td>
<td>glide_list</td>
<td>Specifies users who receive email notifications when the record is updated. By default, only the Incident, Change, and Service Catalog applications notify users listed in this field. For other Task-based applications, you must create custom email notifications sent to the users listed in this field.</td>
</tr>
<tr>
<td>Label</td>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------</td>
<td>---------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Work notes</td>
<td>work_notes</td>
<td>journal_input</td>
<td>Displays and allows the entry of comments viewable only by ITIL users. Each comment is inserted into the Activity field. For more information, see Journal Fields.</td>
</tr>
<tr>
<td>Work notes list</td>
<td>work_notes_list</td>
<td>glide_list</td>
<td>Specifies users who receive email notifications when work notes are added to the record. By default, only the Change, Problem, and Service Catalog applications notify users listed in this field. For other Task-based applications, you must create custom email notifications sent to the users listed in this field.</td>
</tr>
</tbody>
</table>

**Journal fields**

Journal fields work together to create a log of changes and comments as tasks are worked on.

**Note:** Journal fields work on audited tables only.

Fields of the journal_input type are multi-line text boxes which, upon save, add the comments into the Activity field with a notation. If TinyMCE is enabled, you can use it to customize the field text on journal fields.

**Fields that accept input into the journal**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional comments</td>
<td>Any user can update.</td>
</tr>
<tr>
<td>Work notes</td>
<td>ITIL users can update.</td>
</tr>
</tbody>
</table>

These comments, as well as any changes to the record or email notifications sent out because of the record, are displayed in the activity formatter, which can be added to the form like a field.
Activity formatter for journal fields

© 2021 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Planned task

The Planned Task plugin provides a Planned Task [planned_task] table that extends the Task [task] table.

The Planned Task plugin cannot be activated independently. It gets activated when activating the Project Management plugin (through PPM Standard plugin).

Planned tasks provide additional fields for tasks pertaining to time and effort as part of a planned, multi-stage process.

Note: If the Planned Task_v2 (com.snc.planned_taskv2) plugin is active when you upgrade to the Geneva or later releases, the system adds the Task column to the Planned Task [planned_task] table. The Task column is of type Composite Field, and stores the Short Description and Number of the task. During the upgrade, the system updates all records in the Planned Task table.

Create a planned task

Planned Tasks are created on planned task child tables.

Clicking the New button on the Planned Task record list launches the Planned Task Interceptor, which prompts the user to select a child table to create the planned task on:

To modify the planned task interceptor:

1. Navigate to System Definition > Interceptors (this module may need to be activated).
2. Select the Planned Task Interceptor.
3. The Related List **Answers** specifies what choices are presented, and where the user is redirected to once they select the choice. Modify the list as desired.

![Image of the Related List](image.png)

**Create a baseline**

A Planned Task Baseline is a record of the start and end times of the planned task at a particular moment in time.

To create a baseline, navigate to the form of the top planned task and select the **Create a Baseline** related link:
Create baseline

To view the baseline, configure the related lists to add a related list of baselines:
Baselines tab

The baseline can be viewed on a Gantt Chart using the related link.

Measure time and effort

The Planned Task [planned_task] table provides standard fields for tracking duration and effort.

Duration measures the time from start to end date. Effort measures the hours of work exerted on the project.

Duration

- Planned duration: The projected length of time for the planned task.
- Actual duration: The actual length of time so far for the planned task.
- Remaining duration: The Planned duration minus the Actual duration, which represents the projected length of time left.

Effort

- Planned effort: The projected amount of time that will be spent on the planned task.
- Actual effort: The actual amount of time that has already been spent on the planned task.
- Remaining effort: The Planned effort minus the Actual effort, which represents the amount of project work left.
- Percent complete: For the parent task, the percent complete field is not editable and is rolled up from the percent completion of child tasks using the following formula:

  \[
  \text{Percent complete of parent task} = \frac{\text{sum (planned duration of child tasks } \times \text{ percent complete of child tasks)}}{\text{sum (planned duration of child tasks)}}
  \]

  For a child task, the percent complete is entered manually.

Date Calculation: All planned dates and actual dates of the child tasks are rolled up to the parent task automatically. Planned end date for a child task is calculated based on the planned start date and planned duration. If actual start is present, then planned end date is calculated from actual start date and planned duration.

Dependencies: All type of task dependencies, excluding external dependencies, are supported by the planned tasks. For more information about various dependency types, see Project task relationships and dependencies.
## Important planned task table fields

The Planned Task table has these fields.

### Important Planned Task Table Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actual cost</td>
<td>work_cost</td>
<td>currency</td>
<td>The actual cost of the planned task, to be compared with the Estimated cost.</td>
</tr>
<tr>
<td>Actual duration</td>
<td>work_duration</td>
<td>glide_duration</td>
<td>The actual length of time (from start time to end time) of work on the planned task, to be compared with the Planned duration.</td>
</tr>
<tr>
<td>Actual effort</td>
<td>work_effort</td>
<td>glide_duration</td>
<td>The actual time spent working, to be compared to the Planned effort.</td>
</tr>
<tr>
<td>Critical Path</td>
<td>critical_path</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>Estimated cost</td>
<td>cost</td>
<td>currency</td>
<td>An estimation of the cost of the planned task, to be compared with the actual cost.</td>
</tr>
<tr>
<td>HTML Description</td>
<td>html_description</td>
<td>html</td>
<td>A description field that accepts HTML mark-up.</td>
</tr>
<tr>
<td>Percent Complete</td>
<td>percent_complete</td>
<td>decimal</td>
<td>A percentage of the completed effort. Generated using the Planned effort and Actual effort fields.</td>
</tr>
<tr>
<td>Planned duration</td>
<td>duration</td>
<td>glide_duration</td>
<td>The estimated length of time (from start time to end time) of the planned task.</td>
</tr>
<tr>
<td>Planned effort</td>
<td>effort</td>
<td>glide_duration</td>
<td>The estimated amount of time spent working on the planned task.</td>
</tr>
<tr>
<td>Planned end date</td>
<td>end_date</td>
<td>glide_date_time</td>
<td>The estimated date and time for the planned task to end.</td>
</tr>
<tr>
<td>Planned start date</td>
<td>start_date</td>
<td>glide_date_time</td>
<td>The estimated date and time for the planned task to start.</td>
</tr>
<tr>
<td>Remaining duration</td>
<td>remaining_duration</td>
<td>glide_duration</td>
<td>The difference in planned and actual duration, representing the time left for the planned task.</td>
</tr>
<tr>
<td>Label</td>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------</td>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Remaining effort</td>
<td>remaining_effort</td>
<td>glide_duration</td>
<td>The difference in planned and actual effort, representing the amount of work time left for the planned task.</td>
</tr>
<tr>
<td>Rollup</td>
<td>rollup</td>
<td>boolean</td>
<td>Read-only field managed by the system that identifies the task as having child tasks. A rollup task has several its fields calculated from the children so those fields are read-only.</td>
</tr>
<tr>
<td>Time constraint</td>
<td>time_constraint</td>
<td>string</td>
<td>A description of time constraints that apply to the planned task.</td>
</tr>
<tr>
<td>Top Task</td>
<td>top_task</td>
<td>reference (planned_task)</td>
<td>When different planned tasks are stacked in a hierarchy, this field populates with the highest-level parent task. For example, if Project A has a child Project B, and Project B has a child Project C, then the Top Task for Project C is Project A. The Top Task field for Project A is blank.</td>
</tr>
<tr>
<td>Actual start date</td>
<td>work_start</td>
<td>glide_date_time</td>
<td>The actual date when the work starts on the planned task.</td>
</tr>
<tr>
<td>Actual end date</td>
<td>work_end</td>
<td>glide_date_time</td>
<td>The actual date when the work ends on the planned task.</td>
</tr>
</tbody>
</table>

**Planned task scripts**

Several business rules and one script include determines the dynamic calculation of crucial Planned Task fields.

**Planned Task Scripts**

<table>
<thead>
<tr>
<th>Business Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set actual work start value</td>
<td>Sets the Actual Start Date of the planned task when State is set to the default work state.</td>
</tr>
<tr>
<td>Set close data on inactive</td>
<td>Sets the close data of the planned task when task becomes inactive.</td>
</tr>
<tr>
<td>Recalculate</td>
<td>Recalculates the planned task schedule fields when one of the schedule fields changes.</td>
</tr>
<tr>
<td>Planned task global events</td>
<td>Raises global event for every insert or update of planned task record. For more information, see Global events.</td>
</tr>
<tr>
<td>Business Rule</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Update parent actual effort</td>
<td>Rolls up actual effort from child task to parent task.</td>
</tr>
<tr>
<td>Update parent effort</td>
<td>Rolls up planned effort from child task to parent task.</td>
</tr>
<tr>
<td>Update parent percent complete</td>
<td>Rolls up percent complete from child task to parent task.</td>
</tr>
<tr>
<td>Validate duration</td>
<td>Validates the value in the planned duration field is not 0 or negative.</td>
</tr>
<tr>
<td>Validate percent complete</td>
<td>Validates the value in the percent complete field is between 0 and 100.</td>
</tr>
<tr>
<td>Validate work end before work start</td>
<td>Validates that the actual end date is not earlier than the actual start date.</td>
</tr>
<tr>
<td>Set top task</td>
<td>Sets top tasks to maintain hierarchy of tasks.</td>
</tr>
<tr>
<td>Set top task on children</td>
<td>Sets top tasks on child tasks to maintain hierarchy of tasks.</td>
</tr>
</tbody>
</table>

**Planned task hierarchy**

The **Task Hierarchy** tool available for Planned Task displays the relationship between parent and child planned tasks.

Out-of-box, the **Task Hierarchy** tool is available in both Project and Release Management.

Different **Planned Task** tables have different UI actions to launch the task hierarchy:

- To view the hierarchy of a Project, navigate to the use the **Task hierarchy** context menu action.
- To view the hierarchy of a Product in Release v2, navigate to the product and click the **Product hierarchy** related link.
- To view the hierarchy of a Release in Release v2, navigate to the release and click the **Release hierarchy** related link.
Rm2 Hierarchy

The Task Hierarchy can be added to any planned task table by:

1. Navigating to System UI > UI Actions.
2. Selecting one of the existing Task Hierarchy UI Actions (for example, Task hierarchy if Project Management is activated).
3. Change the table to the desired table and rename the UI Action if appropriate, and insert.

The hierarchy should now be available as a UI Action on the form of the new table.

Configure rollup for planned task fields

You can configure the planned task fields to roll up the field values in the parent entity.

By default the following fields are configured to roll up for any planned task and planned task derivatives:

**Cost, Budget, Effort, Actual date, Planned date, Duration, Percent Complete**

1. Navigate to System Definition > Tables.
2. Open the Planned task rollup table.
3. In the Related links, click Show List.
4. Click New.
5. Fill out the Planned task rollup form (see table).
6. Click Submit.

### Planned task rollup form fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Child</td>
<td>Select the table you want to include or exclude.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Field</td>
<td>Select the column name you want to include or exclude.</td>
</tr>
<tr>
<td>Navigator</td>
<td>The reference column of the parent to which the value must be rolled up.</td>
</tr>
<tr>
<td>Parent</td>
<td>Select the parent table.</td>
</tr>
<tr>
<td>Application</td>
<td>Auto-generated value.</td>
</tr>
<tr>
<td>Rollup</td>
<td>Select the check box to allow roll up. Leave the field unchecked to exclude the field from rollup.</td>
</tr>
</tbody>
</table>

**Reminder table**

The Reminder [reminder] table provides a way to auto-generate reminders for a task.

The Reminder [reminder] table is one of the child tables of the Task [task] table. Any table that extends the Task table, such as the Incident [incident] table, can use the Reminder [reminder] table.

Only the system administrator can create or modify a Reminder table. To access the Reminder table, type reminder.do in the filter navigator.

### Reminder table

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task</td>
<td>Refers to the parent task record.</td>
</tr>
<tr>
<td>User</td>
<td>Specifies the user who has logged in to the system.</td>
</tr>
<tr>
<td>Remind me</td>
<td>Specifies the time before which the reminder must be sent. Available values are: <strong>15 minutes, 30 minutes, 1 hour, and 2 hours</strong>. You can add values to this field as required. Note: Internally in the system, the value is always converted to minutes and then stored in the Remind me field.</td>
</tr>
<tr>
<td>Before</td>
<td>Refers to the date from the date field of the parent task record. This date and the time that you mention in the Remind me field are considered to send a reminder. Available values are: Activity due, Due date, Follow up, and SLA due. Note: The Activity due field and the SLA due field are legacy fields with an UNKNOWN value that you cannot use. You can only use the Due date and Follow up fields.</td>
</tr>
<tr>
<td>Using</td>
<td>Specifies the method by which the reminder must be sent. Available options are: <strong>Send an Email</strong> and <strong>Outlook Calendar</strong>.</td>
</tr>
<tr>
<td>Subject</td>
<td>Specifies the subject or the reason of the reminder. Maximum number of characters allowed on this field is 100.</td>
</tr>
<tr>
<td>Notes</td>
<td>Provides a space where you can enter your comments regarding the reminder. Maximum number of characters allowed on this field is 8000.</td>
</tr>
</tbody>
</table>
Task table modifications

Modifications made to the Task table are applied to all child tables.

Be sure that the changes being made are appropriate for all the child tables. Adding fields is a low-impact change, because the field can be hidden on tables that do not need it. However, if the field is being used across tables, deleting fields may cause unwanted data loss.

**Note:** When adding choice list entries to a choice list on the Task table, make sure that the entry value is unique.

You can use dictionary overrides to change some parts of a field definition in a way that does not apply to all child tables.

Tasks workflow

An administrator can specify a specific workflow process to apply to tasks that meet certain conditions.

Once a task is created that meets the conditions, the workflow applies the process to the task, asking for approvals, notifying users, generating other tasks, running scripts, and so on.

Time Card Management

The Time Card Management feature enables time card users such as task assignees to report and track their time for the assigned tasks.

Time Card Management works with the Task table to record time worked on various task types, such as projects, incidents, problems, and change requests.

With the Time Card Management feature:

- The time card users can record the time worked on a task using time cards and time sheets. They can submit their time cards and time sheets for approval.
- Time cards and time sheets are routed for approval based on the Non-project time approver and Project time approver fields in the user time sheet policy. User managers with time card approver role can also log time and submit the time sheet of their resources.
- The time card approvers can perform the following tasks:
  - Review and approve or reject the time cards in a submitted time sheet.
  - Recall the approved time sheets or time cards to return them to the users for corrections.
  - Use dashboards to view reports of time card and time sheet exceptions, and categorize time reported by the users.
  - Delegate another time card approver to process time sheets from your resources when you might not have time or will be unavailable. Note the following points for delegation:
    - You cannot delegate approval only for an individual resource.
    - The delegated time card approver cannot further delegate your time sheet approvals.

The project_manager and the resource_manager roles contain the timecard_approver role in the base system. However, the timecard_approver role can also be used independently without these roles.

- The time card admin can create and manage time sheet policies, and can also approve or reject by exception and process the time sheets. Time card admin can also create or edit time cards of any users if the time cards are in Pending or Rejected state.

Watch this five-minute video to learn about setup of the time tracking feature, entering time and approvals.
**Note:** The Time Card Management plugin is required to use time cards. Some of the procedures require the project management feature, which activates time cards automatically. For more information, see Project Management (com.snc.financial_planning_pmo).

### Domain separation in Time Card Management

Domain separation provides complete data isolation for domain-specific users. Time card Management is domain separation compliant at the **Data only** level.

### Activate Time Card Management

Administrators can activate the Time Card Management plugin (com.snc.time_card). The plugin also activates the Performance Analytics - Content Pack - Project Portfolio Suite Dashboards plugin (com.snc.pa.time_card). However, you need a Performance Analytics license to use the dashboards.

Role required: admin

**Note:** The Time Card Management plugin also gets activated as part of PPM Standard plugin (com.snc.financial_planning_pmo).

1. Navigate to **System Applications > All Available Applications > All**.
2. Find the plugin using the filter criteria and search bar.
   
   You can search for the plugin by its name or ID. If you cannot find a plugin, you might have to request it from ServiceNow personnel. For more information, see Request a plugin.
3. Click **Install**, and then in the Activate Plugin dialog box, click **Activate**.

**Note:** When domain separation and delegated admin are enabled in an instance, the administrative user must be in the **global** domain. Otherwise, the following error appears: Application installation is unavailable because another operation is running: Plugin Activation for <plugin name>.

### Time sheet policies

Time sheet policies contain the policies to which a time sheet, or a time card must adhere.

By default, the Default time sheet policy is available with the system. As a Time card admin, you can create multiple time sheet policies based on different requirements and workflows in your organization. For example, specify a time sheet policy for each department or team and assign appropriate users to them.

Time sheet policies also provide an ability to specify appropriate approval workflow for project and non-project tasks.

A time sheet policy can be **set as a default policy**. The default policy is a global time sheet policy which applies to all the users who are not assigned to any other time sheet policy. Only one time sheet policy can be set as a default policy.

Navigate to **Time Sheets > Administration > Time Sheet Policies** to view the list of timesheet policies.

#### Create a time sheet policy

As a time card administrator, you can create a time sheet policy to define the requirements for time card users to record their time worked. The time card approvers must review and process time sheets under the applicable time sheet policy.

Role required: timecard_admin

1. Navigate to **Time Sheets > Administration > Time Sheet Policies**.
2. Click **New**.
3. On the form, fill in the fields.

**Time Sheet Policy form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name of the policy.</td>
</tr>
<tr>
<td>Allow blank time cards</td>
<td>Option to enable submission of blank time cards for approval. By default, this option is not selected.</td>
</tr>
</tbody>
</table>
| Auto create time card on planned task update  | Option to create a time card automatically when you update a planned task, if the following conditions are true:  
  • You are a time card user  
  • You are assigned to the task through **Assigned to** or **Additional assignee list** field  
  • The task is not in a pending state. By default, this option is not selected. |
| Auto fill time card with time worked entries  | Option to fill in time cards automatically when you enter time in the **Time worked** field on the Task form.  
  If a time card does not exist for the task, one is created when the time worked is updated if the following conditions are true:  
  • You are a time card user.  
  • You are assigned to the task through the **Assigned to** or **Additional assignee list** field. By default, this option is not selected. |
<p>| Auto create time cards every week             | Option to <strong>generate time cards automatically</strong> every week through a scheduled job for all users assigned to the time sheet policy. The time cards are generated based on the planned task assignments and hard-allocated resource plans of the users. By default, this option is selected. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Update actual hours and cost in resource plan/reports | Option to update actual hours and actual cost of the associated resource plan based on the hours entered in the approved time card. When selected, you can associate a resource plan related to the selected task with the time card in the following ways:  
  • If the task has multiple resource plans, you can select the appropriate plan.  
  • If the task has one resource plan, that plan is selected by default.  
  The hours from the time card entry and the hourly resource rate are used to update the **Actual hours** and **Actual cost** values of the associated resource plan.  
  **Note:** If the task has no resource plan, the associated records update the corresponding project.  
  By default, this option is not selected. |
| Allow recall                               | Option to enable the recall action on a time sheet or time card after it is approved and processed. By default, this option is selected.                                                                     |
| Recall period allowed (days)              | Number of days within which you can recall a time sheet or time card.  
  This field appears when the **Allow recall** option is selected.  
  The default value is 30.                                                                 |
| Week starts on                             | Start day of the week for the time sheet. The default value is Sunday.                                                                                                                                 |
| Maximum hours per day                     | Maximum number of hours that can be entered each day in a time sheet.  
  If set to -1, the resource can enter a value from 0 through 24 for the hours worked each day.  
  The default value is 24.                                                                 |
| Maximum hours per week                    | Maximum number of hours allowed in a week in a time sheet.  
  The value for total hours for a week in a time sheet is the sum of hours entered per day of that week. If set to -1, the total hours per week allowed is up to 168 (24 x 7) hours.  
  The default value is 40.                                                                 |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-project time approver</td>
<td>Type of approval required when you submit a time card that has a non-project task assigned.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto</strong>: Time card is auto-approved when submitted.</td>
</tr>
<tr>
<td></td>
<td>• <strong>User Manager</strong>: Time card is routed to the user manager for approval when submitted.</td>
</tr>
<tr>
<td></td>
<td>The user manager has the time card approver role and is also selected as the manager of the time card user on the User form.</td>
</tr>
<tr>
<td></td>
<td>• <strong>None</strong>: A user with the timecard_admin role can approve time cards when submitted.</td>
</tr>
<tr>
<td>Project time approver</td>
<td>Type of approval required when you submit a time card that has the project task.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto</strong>: Time card is auto-approved when submitted.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Project Manager</strong>: Time cards for a project task are routed to the respective project manager for approval when submitted. The project manager is picked from the task against which you are submitting time.</td>
</tr>
<tr>
<td></td>
<td>• <strong>User Manager</strong>: Time cards are routed to the user manager for approval when submitted.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Both</strong>: Time cards are routed to both the user manager and project manager for approval when submitted.</td>
</tr>
<tr>
<td></td>
<td>A time card remains in the Submitted state when only one of the approvers approves the time card.</td>
</tr>
<tr>
<td></td>
<td>• <strong>None</strong>: A user with the time_card admin role can approve time cards.</td>
</tr>
</tbody>
</table>

**Note:**
- The project manager and the user manager can view only those time cards that are routed to them for approval.
- If the user manager or the project manager changes while the time card is still not approved, the system automatically updates the approver of the time card.
- If the name of the project manager or the user manager is not populated on the respective form, a user with the time_card admin role can approve time cards.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow multiple rate types</td>
<td>Option to provide a rate type in a time card to be used during expense line generation. When this option is selected, the Rate type field displays on the Time Card form to enable the selection of a rate type. For more information, see Rate type in labor rate card.</td>
</tr>
<tr>
<td>Default rate type</td>
<td>Rate type used by default for the time card. If you select none, the Standard rate type option is used. This field appears when the Allow multiple rate types check box is selected.</td>
</tr>
<tr>
<td>Default Policy</td>
<td>Option to set the time sheet policy as the default. The default policy is a global time sheet policy that applies to all users who are not assigned to any other time sheet policy. Only one time sheet policy can be set as the default. A time sheet policy set as the default policy cannot be deleted. You must first set another policy as the default policy.</td>
</tr>
</tbody>
</table>

4. Click Submit.

- Set the time sheet policy as the default policy, if required.
- Assign the time sheet policy to users.

**Set a time sheet policy as default policy**

As a time card administrator, you can set a time sheet policy as the default policy. The default policy is a global time sheet policy which applies to all the users who are not assigned to any other time sheet policy.

Role required: timecard_admin

Only one time sheet policy can be set as a default policy.

1. Navigate to Time Sheets > Administration > Time Sheet Policies.
2. Open the time sheet policy record.
3. Click the Set as default related link.

**Note:** The related link appears only for a time sheet policy which is not already set as the default policy.

The Default Policy option on the record form is selected to indicate that the current time sheet policy is set as the default policy. The Default Policy option on the earlier default time sheet policy is cleared.

You cannot delete a default time sheet policy. You must first mark another policy as the default policy to delete the current default policy.

**Assign a time sheet policy to a user**

As a time card administrator, you can assign a time sheet policy to a user.

Role required: timecard_admin
You can assign only one time sheet policy to a user.

1. Navigate to Time Sheets > Administration > Time Sheet Policies.
2. Open the time sheet policy record.
3. In the Users related list, click Edit.
4. On the Edit Members form, move the users to the User List.
5. Click Save.

The selected users appear on the Users related list. The time sheet policy is assigned to the selected users.

Create a rate type

You can create rate types using the Rate Types feature.

Role required: timecard_admin

The rate type functionality is used to categorize different types of work. For example, Standard versus Overtime. It can also instruct down-stream, third-party product about the nature of the work performed.

For example:

- A user works extra time during the day and must differentiate standard time from overtime.
- A technician may be paid at a higher rate based on different types of work involved in the execution of a task.
- An appliance repair task may be billed at one rate for the first hour and a different rate for the remaining hours.
- A service call may last four hours during which specialized equipment is used for one hour. The company must capture the use of the specialized equipment for purposes ranging from additional billing to legal compliance or warranty tracking.

1. Navigate to Time Sheets > Administration > Rate Types.
2. Click New and fill the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Provide a suitable name for the rate type.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Summarize the purpose of the rate type.</td>
</tr>
<tr>
<td>Active</td>
<td>Deselect the check box to mark the rate type as inactive.</td>
</tr>
</tbody>
</table>

3. Click Submit.

- The rate type is displayed in the Rate Types list.
- The rate type if active is also displayed in the Rate Type field in the Labor Rate Cards form, Time Worked form, Time Card form, and Time Sheet Portal.

Time Sheet Portal

Time Sheet Portal categorizes and displays all your assigned tasks in a single view for a given week. The portal enables you to record time spent on tasks on a day-to-day basis and submit the time sheet in a single action.

Time Sheet Portal works with the Task table to record the time that you spend on various task types, such as projects, incidents, problems, and change requests. It provides a complete breakdown of the time you enter for the task, task categories, and days in a week. It enables you to:
- Generate time cards for assigned projects or project tasks.
- Copy time cards from a previous time sheet.
- Search and create a time card for a task that is not displayed in the assigned tasks list.
- Edit, delete, or add notes to a time card.
- Submit, approve, reject, and recall a time sheet.
- View notifications for the submitted, rejected, and recalled time sheets or time cards.

Time Sheet Portal comprises of the following sections:

**Header**

![My Time Sheet]

The Time Sheet Portal header:

- Displays a date range of the time sheet for the selected week and provides options to navigate to the time sheet of previous or next week.
- Provides a calendar along with the date range. Clicking a date in the calendar displays the time sheet for the week of the selected date.
- Provides a link to navigate to the time sheet for the current week when a different time sheet is being viewed.
- Provides an option under *My Time Sheet* that enables you to open and edit the time sheets of your resources. The option is available only for a user manager.

- Provides an option to view the time sheet in the Form view using time sheet form view icon ( ).
• Displays the notifications for the submitted, rejected, and recalled time sheets under the show notifications icon (1). Each entry displays the number of time cards and their state. Click on a notification item to open the time sheet.
Tasks

The **Tasks** tab displays your assigned tasks as cards. Each card provides information about a task, such as short description, state, last updated date and time, and priority. Tasks are derived from the following filter conditions:

- All your assigned incidents, problems, or change requests that are active.
- All your assigned incidents, problems, or change requests that are closed in the selected week.
- All tasks for which you are hard-allocated during the selected week.
- All your assigned projects or project tasks that are active during the selected week. Project or project tasks are derived from the following conditions:
  - A project or project task that has started and its actual start date is before the end of the selected week.
  - A project or project task has closed and its actual end date is after the week has begun.
  - When there are no actual dates for a project, planned dates of the project must occur within the selected week.
- All active stories assigned to you.
- All active scrum tasks assigned to you or closed in the selected week.
- All active test plans assigned to you.
• All active defect and enhancements assigned to you or closed in the selected week.

**Note:** If the Customer Service Management plugin (com.sn_customerservice) is activated, your assigned tasks that are active and closed in the selected week are also derived from the following tables:

- Case [sn_customerservice_case]
- Work Order [wm_order]
- Work Order Task [wm_task]

On the **Tasks** tab, you can perform the following operations:

• Type a keyword in the search field to view only cards with details that match the keyword.
• Sort cards in ascending or descending order based on priority, irrespective of the task type.
• View cards based on a category, such as projects, project tasks, incident, problem, change, defect, enhancement, test plans, and scrum tasks.
• **Create time cards** for assigned tasks.

**Note:** Time sheet policies apply when you create or edit a time card.
The **Group Tasks** tab displays the tasks assigned to your **Assignment group**. The group tasks are displayed as cards in the tab. A card provides information about the task, such as short description, state, last updated date and time, and priority.
The **Other** tab displays cards used to log time for operational work, such as administration, meeting, and KTLO.

**Note:** The list of categories in the time card controls the list of cards displayed on the **Other** tab. If an administrator marks any of the categories as inactive in the time cards, those categories are not displayed on the **Other** tab.
The Time Sheet section:

- Displays the date range of the time sheet for the selected week.
- Indicates the state of the time sheet being viewed.
- Displays the total number of tasks and hours that you have entered for each day in a week. When you click a day in the time sheet, the column for that day is highlighted in both the Time Sheet and Logged Time Cards sections. The first day displayed in the Time Sheet section is based on the value specified in the Week starts on field in the users Time Sheet Policy. For example, if the Week starts on field is set to Friday, the Time Sheet section starts with Friday.
- Indicates the total number of hours that you entered in the time sheet. Time Sheet breakdown also displays a breakdown of user-entered hours in different work categories, such as project tasks, admin, meeting, follow on tasks, or change requests.
- Provides options that enable you to submit a time sheet and copy time cards from a previous time sheet. For an approver, options to approve or reject a submitted time sheet and recall a processed time sheet are available.
Logged Time Cards

Each row in the Logged Time Cards section represents a time card entry for a given week. It has details such as icon for state of the time card, short description of the task, project time category, rate type, resource plan, and logged time. Each row of the time card contains options that enable you to edit, delete, or add notes to a time card. For more information, see Create time cards and log time through Time Sheet Portal.

<table>
<thead>
<tr>
<th>Short description</th>
<th>Project time category</th>
<th>Rate type</th>
<th>Resource plan</th>
<th>Sun</th>
<th>Mon</th>
<th>Tue</th>
<th>Wed</th>
<th>Thu</th>
<th>Fri</th>
<th>Sat</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>Sales Requests...</td>
<td>Develop...</td>
<td>None</td>
<td>RPLN000...</td>
<td>0</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>12</td>
</tr>
<tr>
<td>Security Review...</td>
<td>None</td>
<td>None</td>
<td>RPLN002...</td>
<td>0</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>0</td>
<td>20</td>
</tr>
<tr>
<td>Apply patch...</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>5</td>
</tr>
</tbody>
</table>

**Note:**
- The **Rate type** column is visible only when the **Allow multiple rate types** option in the time sheet policy of the user is selected.
- The **Resource plan** column is visible only when the **Update actual hours and cost in resource plan/reports** option in the time sheet policy of the user is selected.

The icon beside the short description of a row indicates a time card state. The merge icon in a time card row indicates that a duplicate time card for the same task exists in the time sheet and provides option to merge them into a single time card.
When there are no time cards, the Logged Time Cards section displays the **Generate Time Cards** and **Copy from previous time sheet** buttons to create time cards.

**Create time cards and log time through Time Sheet Portal**
After you create time cards in Time Sheet Portal, log time in the time cards.

Role required: timercard_user

1. Navigate to **Time Sheets > Time Sheet Portal**.
2. Create time cards in the **Logged Time Cards** section using any of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Steps</th>
</tr>
</thead>
</table>
| **Generate time cards for assigned projects or project tasks** | a. Click choice list next to **Submit**.  
   b. Select **Generate Time Cards**. The option also appears in the **Logged Time Cards** section when a user has no time cards for the selected week.  
   
   **Note:**  
   • If a time card exists for a project task during the selected week, a duplicate time card is not created.  
   • Time cards are generated only for those project tasks that are in progress or planned for the selected week.  
   • The **Allow time card reporting on** field on the project form determines the level at which the time cards are created for project tasks. |

| **Copy time cards from a previous time sheet** | a. Click choice list next to **Submit**.  
   b. Select **Copy from previous Time Sheet**. The option also appears in the **Logged Time Cards** section when a user has no time cards for the selected week.  
   
   **Note:**  
   • Time cards for all the project tasks that are in progress or planned in the current week are copied from the selected time sheet. If a time card for a project task exists, a duplicate time card is not created while copying.  
   • Time cards for all the non-task categories, such as meetings and trainings, are copied from the selected time sheet. If a time card for a non-task category exists, a duplicate time card is created while copying. |
<table>
<thead>
<tr>
<th>Option</th>
<th>Steps</th>
</tr>
</thead>
</table>
| Create a time card from the Tasks, Group Tasks, or Other tab | a. On the Tasks, Group Tasks, or Other tab, point to a task (card) that you want to create a time card for.  
   b. Click Add to Time Sheet. |
|                                             | Note: Add to Time Sheet creates a time card with the default rate type of the user, if it exists. |
| Create multiple time cards from the Tasks tab | a. On the Tasks tab, select multiple tasks that you want to create time cards for.  
   b. Click Add selected to Time Sheet. |
| Create a time card for unassigned task       | a. In the Logged Time Cards section, click Add unassigned tasks to Time Sheet.  
   b. Enter the task number or short description of the task you worked on during the selected week. |

Based on the Allow time card reporting on field settings in the Preferences tab of a project, the Add to Time Sheet and Add selected to Time Sheet options are displayed in Time Sheet Portal.

3. In the Logged Time Cards section, log time in a time card:

<table>
<thead>
<tr>
<th>Option</th>
<th>Steps</th>
</tr>
</thead>
</table>
| Through inline editing        | a. Select a row and press Enter. You can also double-click a row.  
   b. Edit the values as required. |
| Through time card form        | a. Point to a row and click the more actions icon  
   b. To open the Time Card form, click Open Form View.  
   c. Enter hours on the time card form.  
   d. Click Save. |
| Add notes to time cards       | a. Point to a row and click the more actions icon.  
   b. To add a note, click Add Note. |

Submit time sheet through Time Sheet Portal
Once you update the time sheet with time worked for a given week, submit it for approval.

Role required: timecard_user

When you submit a time sheet, time cards are verified against the assigned time sheet policy. If there is no time sheet policy assigned, time cards are verified against the default time sheet policy. Business rules prevent you from submitting a time sheet in case any violation is found.

1. Navigate to Time Sheets > Time Sheet Portal.
2. Click **Submit**.
   The time sheet moves to the Submitted state.

**Log time and submit time sheets of your resources**
As a user manager, you can log time and submit the time sheet of your resources.

A user manager must have time card approver role to create and edit time cards, and submit the time sheet of other time card users. The user manager has either of the required roles and is the one listed as the manager of the time card users.

Role required: timecard_approver

1. Navigate to **Time Sheets > Time Sheet Portal**.
2. Click **My Time Sheet** choice list and select the user for whom you want to approve or reject time sheet for under **My Resources**.

   The **My Resources** section lists the time card users reporting to you.

   **Note:** The choice list with **My Time Sheet** is available only for a user manager.

3. Create time cards and log time as required.
4. Click **Submit**.

   • The time sheet of the selected user moves to the Submitted state. The time sheet policy assigned to the time card user is used for validation when you submit the time sheet.
   • All the time cards associated with the time sheet are also submitted automatically and move to the Submitted state.
   • The **Approve** and **Reject** buttons appear in the Time Sheet section. The two buttons appear only for a user manager.

Once you have submitted the time sheet for your resource, you can click **Approve** or **Reject** to approve or reject it. Only the time cards that are routed to the user manager, are approved or rejected. The routing for approval happens based on the **Non-project time approver** and **Project time approver** fields in the time sheet policy of the time card user.

**Time Sheets**
A time sheet groups all the time cards for a user for the given week.

With time sheets:
• Time card users can submit all the time for their work week in a single step by using a time sheet.
• Time card approvers can approve all the time cards in a time sheet for a user in a single step by approving the time sheet. They do not need to approve multiple time cards for a given user individually.
• Track the activities of a time sheet, such as who submitted or approved a time sheet, in the Activities section on the Time Sheet form. This time sheet activity audit is useful for tracking when you delegate responsibility for your time card processing to another user. To track the activities, enable the **State** field of the Time Card [time_card] table for auditing the time card activities, if it is not already enabled. For more information, see Include a table field in auditing.

A time sheet can have any of the following states:
• Pending
• Submitted
• Approved
• Processed
• Rejected
• Recalled
Create a time sheet
As a time card user, you can create a time sheet to group all your time cards for the given week and submit them in a single step.

Role required: timecard_user
A user can create only one time sheet per week.

Note: When a user creates a time card for a week, a time sheet is also automatically created for that week.

1. Create the time sheet with one of these options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>From the time sheet menu</td>
<td>Navigate to Time Sheets &gt; My Time Sheets &gt; Current (This Week). The time sheet form for the current week opens.</td>
</tr>
<tr>
<td>From the time sheet list</td>
<td>a. Navigate to Time Sheets &gt; My Time Sheets &gt; All &gt; New. b. Click New.</td>
</tr>
</tbody>
</table>

2. On the form, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Week starts on</td>
<td>Starting date of the week for which the time sheet is created.</td>
</tr>
<tr>
<td>Note:</td>
<td>The time sheet policy Week starts on controls the start day of the week.</td>
</tr>
<tr>
<td>Total Hours</td>
<td>Number of hours the user has worked in that week. This field is automatically populated from the hours recorded for the associated time cards.</td>
</tr>
<tr>
<td>User</td>
<td>Name of the user for which time sheet is created.</td>
</tr>
<tr>
<td>State</td>
<td>Current state of the time sheet. All new time sheets begin as Pending. Default states: Pending, Submitted, Approved, Processed, and Rejected.</td>
</tr>
<tr>
<td>Comments</td>
<td>Comments related to the time sheet.</td>
</tr>
<tr>
<td>Notes</td>
<td>Any additional information.</td>
</tr>
</tbody>
</table>

3. Click Submit.
Add time cards to the time sheet. You can use the related links and related list to add time cards. You can also add time cards using the Time Sheet Portal.
Submit a time sheet
Once the time sheet is updated with time worked, you can submit the time sheet for the week to submit all the time cards for the week together.

Role required: timecard_user

When a user submits a time sheet, the time sheet policy assigned to the user is used for validation. If there is no time sheet policy assigned to the user, the default time sheet policy is used. Business rules prevent a user from submitting a time sheet in case any violation is found.

Note: You can also perform this task from the Time Sheet Portal.

1. Navigate to the time sheet using one of the following options:
   • To submit a time sheet in the Pending state, navigate to **Time Sheets > My Time Sheets > Pending**.
   • To submit the time sheet for the current week, navigate to **Time Sheets > My Time Sheets > Current Time Sheet**.
   • To submit a time sheet in the Rejected state, **Time Sheets > My Time Sheets > Rejected**. You can make required changes as suggested in the rejection comments to resubmit a rejected time sheet.

2. To submit in the Time Sheets list, open the time sheet.
3. Add comments, if required.
4. Click **Submit Time Sheet**.

   • The time sheet moves to the Submitted state.
   • All the time cards associated with the time sheet are also submitted automatically and move to the Submitted state.

Approve or reject a time sheet
As a user manager, you can view and approve or reject a time sheet to approve or reject all the time cards for a user for the given week in a single step.

Role required: timecard_approver or timecard_admin

A user manager is the one who has either of the required roles and is selected in the Manager field on User form of the time card user.

During out-of-office time, the user manager can delegate another user with the required roles as the time sheet approver. For the specified time period, the delegated user also receives all the time sheets submitted by the time card users to process.

1. Navigate to **Time Sheets > Time Sheets > Pending Approval**.
2. In the Time Sheets list, open the time sheet to approve or reject.
3. If required, add comments.
4. Click Approve or Reject.

- The time sheet moves to the Approved or Rejected state.

**Note:** If a time sheet is rejected, it gets listed in the notifications for the rejected time sheets under the show notifications icon on Time Sheet Portal.

- All the time cards associated with the time sheet are also approved or rejected automatically.
- If any time cards in the time sheet are pending approval by one of the approvers as defined by the time sheet policy, the time sheet remains in the Submitted state.

**Note:**
- You can also approve or reject the time cards within a time sheet selectively by selecting one or more time cards and approving or rejecting them.
- If a time sheet is rejected, all the associated time cards in the Submitted state are also rejected automatically. The time cards in the Approved and Processed state for the time sheet remain unaffected.
- If all the time cards in a time sheet are approved, the time sheet automatically moves to the Approved state.
- If a time card in a time sheet is in the Rejected state, then irrespective of the state of other time cards in the time sheet, the time sheet also moves to the Rejected state.

**Time cards**

Time cards are used to record the time worked on a task by a task assignee.

The time card management feature works with the Task table to record time worked on Projects, Incidents, Problems, and Change Requests.

Task assignees can record time worked in the **Time worked** field on a task record or enter hours directly into their time card. Some tables support automatic time card creation based on start and end date fields.

Track the activities of a time card, such as who submitted or approved a time card, in the Activities section on the Time Card form. This time card activity audit is useful for tracking when you delegate responsibility for your time sheet processing to another user. To track the activities, enable the **State** field of the Time Card [time_card] table for auditing the time card activities, if it is not already enabled. For more information, see Include a table field in auditing.

You can associate time cards for the project tasks and other task categories, such as meeting and training, with relevant resource plans.

When you approve a time card, the time logged in the time card is saved day-wise in the Time Card Daily [time_card_daily] table. Using daily time logged data, you can generate time card reports by days for any period irrespective of the time sheet period to which the time cards belong. For example, you can create monthly time card report that includes time cards from the first day to the last day of the month.

Time cards also have an optional approval mechanism for project managers to approve the time cards. Administrators and time card approvers can see all the time cards for the week. All users who are in a role that is responsible for working on tasks also can access their personal time cards. A time card can have any of the following states:

- Pending
- Submitted
- Approved
Create a time card
You can create time cards to log time against the work you have done.

Role required: timecard_user

The **Allow time card reporting on** field on the **project form** determines the level at which the time cards for the project tasks can be created.

Time cards can be created automatically or manually.

- **Automatic**: Use the following options to automatically generate the time cards:
  - **By updating task**:
    - **Auto create time card on task update**
      Configure time cards to be created when a user updates a task record. The **Auto create time card on task update** setting in the assigned **time sheet policy** controls this behavior and is set to false by default.
    - **Auto fill time card with time worked entries**
      Configure time cards to be created when a user records **Time worked**. A time card is created if a time card does not exist for the task. The time sheet policy **Auto fill time card with time worked entries** controls this behavior and is set to false by default.

      In **Project Task**, **Incident**, **Problem**, and **Change** records, the **Time worked** field does not appear by default and must be configured on the form.

  - **By scheduled job**: Configure time cards for the project tasks to be generated automatically for users through a **scheduled job**. Only the admin can configure a scheduled job.

- **Manual**: Create a time card for each task and enter the time manually.

1. Create the time card using one of the following options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>From the Time Sheet Portal</strong></td>
<td>a. Navigate to <strong>Time Sheets &gt; Time Sheet Portal</strong>.</td>
</tr>
<tr>
<td></td>
<td>b. Open the week on the <strong>Calendar</strong> for which you want to create the time card.</td>
</tr>
<tr>
<td><strong>From a Time sheet related list</strong></td>
<td>a. Open the time sheet that you want to create the time card for.</td>
</tr>
<tr>
<td></td>
<td>b. In the <strong>Time Cards</strong> related list, click <strong>New</strong>.</td>
</tr>
</tbody>
</table>
Option | Steps
--- | ---
From a Time sheet related link | 

a. Open the time sheet for which you want to create the time card.

b. Click any of the following related links:

- **Generate Time Cards**: This option generates the time cards for all project tasks assigned to the user for the time sheet week. With this option, time cards are generated only for the project tasks that are in progress or planned in that week.

- **Copy from previous time sheet**: This option copies all the time cards (for project and non-project tasks) from a selected time sheet.

**Note:**

When using the related links for creating time cards:

- If a time card exists for a project task for the time card week, a duplicate time card is not created.

- Time cards are generated only for those project tasks that are in progress or planned in that week.

2. On the form, fill in the fields.

**Time card form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Week starts on | Starting date of the week of the time sheet. 

**Note:** The time sheet policy Week starts on controls the start day of the week. |
| State | Current state of the time card. All new time cards begin in the Pending state.  
Different states of a time card are Pending, Submitted, Approved, Processed, Rejected, and Recalled. |
| Category | Type of task for which the time card is created. |
| Task | Task that is associated to the time card. |
| Project time category | Type of activity in the project that time is reported for.  
This field appears when you select Project/Project Task or Task work in the Category field. |
| User | Name of the user that the time card is created for. |
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate type</td>
<td>Rate type that is considered during the expense line generation. For more information, see Rate type in labor rate card.</td>
</tr>
<tr>
<td>Note:</td>
<td>This field appears when the Allow multiple rate types option is selected in the assigned time sheet policy of the user.</td>
</tr>
<tr>
<td>Resource Plan</td>
<td>Resource plan of the task associated with the time card. When the time card is approved, the hours from the time card entry and the hourly resource rate are used to update the Actual hours and Actual cost values of the associated resource plan. A resource plan is associated with the time card in the following ways:</td>
</tr>
<tr>
<td></td>
<td>• If the task has multiple resource plans, you can select the appropriate plan.</td>
</tr>
<tr>
<td></td>
<td>• If the task has one resource plan, that plan is selected by default.</td>
</tr>
<tr>
<td>Note:</td>
<td>If the task has no resource plan, the associated record updates the corresponding project.</td>
</tr>
<tr>
<td></td>
<td>This field appears when the Update actual hours and cost in resource plan/reports option is selected in the assigned time sheet policy of the user.</td>
</tr>
<tr>
<td>Remaining effort</td>
<td>Amount of work time left for the planned task. Remaining effort is the remaining effort in the planned task table and is calculated as: Remaining effort = Planned effort - Actual effort</td>
</tr>
<tr>
<td>Note:</td>
<td>The field is not available on the Time Card form by default. Configure the form to add this field if required.</td>
</tr>
</tbody>
</table>

3. Click Submit.

- The time card is created for the selected time card period.
- If the time sheet for the week does not exist, a time sheet is created for the time card week.

After the time card is created, the hours for that task can be incremented automatically from the Time worked field in the task record. The time sheet policy Auto fill time card with time worked entries controls the way the time is updated in time cards. The policy is set to false by default. If automatic updates for time worked are not configured, the user must manually update the time card.

Copy time cards from a previous time sheet.
Another option for creating time cards is to copy them from an existing timesheet, which copies all the time cards (for project as well as non-project tasks) from a selected time sheet.

Role required: timecard_user

You can also perform this task from the Time Sheet Portal.

1. Open the time sheet record that you want to create the time cards for.
2. Click the Copy from previous time sheet related link.
3. In the Select Time Sheet field, select a previous time sheet that you want to copy the time cards from.
4. Optionally, if you want to copy the time logged for the tasks in the previous time sheet, select the Copy time logged check box.
5. Click OK.

**Time cards for project tasks**

Time cards for all the project tasks that are in progress or planned in the current week are copied from the selected time sheet. If a time card for a project task exists, a duplicate time card is not created during copying.

**Time cards for non-task category**

Time cards for all non-task category such as meetings and trainings are copied from the selected time sheet. If a time card for a non-task category exists, a duplicate time card is created during copying.

- If the previous time sheet has rate types and the time sheet policy of the user allows rate types, then rate types are also copied into the current time sheet.
- If the previous time sheet has rate types, but the time sheet policy of the user no longer allows rate types, then rate types are not copied to the current time sheet.
- If the previous time sheet has a rate type that is inactive, that rate type is not copied. If necessary, the user can enter a different rate type before saving the individual time cards.

**Auto-generate time cards**

As an admin, you can configure a scheduled job to generate time cards automatically for project tasks assigned to time card users.

Role required: admin

In addition to the manual option Generate Time Cards, a scheduled job can be run to automatically generate the time cards for project tasks. A job can be scheduled to run every week, for example, on every Sunday to generate timesheets for all users for the next week. You can configure when to run the scheduled job based on the business process of the organization. By default, the scheduled job is turned off. For more information, see Schedule a script execution.

**Note:** The scheduled job auto-generates time cards only for those users who have the Auto create time cards every week option set to true in their assigned time sheet policy.

1. Navigate to System Definition > Scheduled Jobs.
2. In the Scheduled Jobs list, select Auto Generate Time Cards.
3. Configure the following parameters in the script as per the business requirements:
   - run for (CURRENT_WEEK, NEXT_WEEK, LAST_WEEK)
   - Group Name (includeGroups, excludeGroups)

**Note:**
• If a time card exists for a project task for the time card week, a duplicate time card is not created.
• Time cards are generated only for those project tasks that are in progress or planned in that week.
• The **Allow time card reporting on** field on the project form determines the level that the time cards for the project tasks are created at.

The following example script is executed when a scheduled job is run to generate time cards for the **Current week** for the **Database** and **Hardware** groups:

```javascript
// Clone this schedule job to run separately for different groups at different times
// One of the following values
// TimeCardConstants.CURRENT_WEEK
// TimeCardConstants.NEXT_WEEK
// TimeCardConstants.LAST_WEEK
var runFor = TimeCardConstants.CURRENT_WEEK;

// Comma separated group sys ids or group names. TimeSheet/TimeCards will be auto generated for time card users in the given groups.
var includeGroups = [Database, Hardware];
var excludeGroups = [];

var generator = new TimeCardGenerator();
generator.generateFromConfig(runFor, includeGroups, excludeGroups);
```

**Submit a time card**

As a time card user, once a time card for the week is updated with the time worked, you can submit the time card individually.

A time card in the Pending or Rejected state can be submitted.

Role required: timecard_user

When a user submits a time card, the **time sheet policy** assigned to the user is used for validation. If there is no time sheet policy assigned to the user, the default time sheet policy is used. Business rules prevent a user from submitting a time card in case any violation is found.

1. Navigate to:
   • **Time Sheets > My Time Cards > All**
   • The **Time cards** related list in a time sheet.

   **Note:** You can select multiple time cards to submit.

2. In the Time Card list, open the time card to submit.
3. Click **Submit Time Card**.

   • The time card moves to the Submitted state.
   • The time card is submitted to an approver based on the values set in the **Project time approver** and **Non-project time approver** fields in the time sheet policy assigned to the user.

   **Note:** If the project or user manager is changed after submitting the time card, the time card is automatically redirected to the new project or user manager for approval.
Approve or reject a time card
As a time card approver, you can view and approve or reject a submitted time card.

Role required: timecard_approver or timecard_admin

You can view only those time cards that are submitted to you for approval or you have been delegated as the time card approver by one of the other user managers. The time sheet policy assigned to the user governs the approval process.

1. Navigate to Time Sheets > Time Cards > Pending Approval.
2. Select the time card to approve or reject.
3. Click Approve or Reject.

- The time card moves to the Approved or Rejected state.
- For an approved time card, a Time Card Daily record is created.

Note:
- A user manager can also approve the time cards within a time sheet by selecting one or more time cards and approving them. When all the time cards in a time sheet are approved, the time sheet automatically moves to the Approved state.
- A user manager is one who is selected in the Manager field on User form of the time card user.
- If a time card is in the Rejected state, the associated time sheet also moves to the Rejected state irrespective of the state of other time cards in the time sheet.

Record time worked
The time card retrieves time accrued on a project or spent working on any record in the Task table from the Time worked field.

This field does not appear by default on the Project Task, Incident, Problem, and Change forms and must be added by personalizing the form. Time recorded in this field is used to populate an existing time card or to create a new time card if one does not exist. A time sheet policy controls this behavior.

Note:
- When time worked is updated, a time card is created only if:
  - the user is a time card user, AND
  - the user is assigned to the task through Assigned to or Additional assignee list field.

The Time worked field has a counter that acts like a stopwatch for the duration of the time spent in the record. A button in the field can stop and start the counter. By default, the Time worked counter is enabled and begins
recording the elapsed time when the record is opened. Stop the counter with the stop button and restart it with the play button.

Time counter started:

![Time worked](image)

**Time worked started**

Time counter stopped:

![Time worked](image)

**Time worked stopped**

If you are creating time cards from time worked entries, you can ask your admin to add the Time Worked related list to display the time worked records on the time card form. You will also notice an informational message on the time card to let you know that changes to time worked records overrides values in the time card. This is displayed using a **formatter**, which can be added or removed by configuring the form.

If you are creating time cards from time worked entries, you can ask your admin to add the Time Worked related list to display the time worked records on the time card form. You will also notice an informational message on the time card to let you know that changes to time worked records overrides values in the time card. This is displayed using a **formatter**, which can be added or removed by configuring the form.

**Manage costs**

When the cost management feature is enabled, time cards can be used to manage the cost of labor in the Cost Management application.

When a time card for a project task is approved, an expense line is generated for the corresponding labor cost associated with the project. If the project has a rate model associated, then the hourly rate for calculating labor cost for the expense lines is derived from the rate model. If no rate model is associated to the project, the rate listed in the **Labor Rate Card** is considered. If no Labor Rate Cards is applicable, the property **com.snc.time_card.default_rate** defines the default hourly rate.
Roles

The timecard_admin role enables users to approve, modify, and delete the time cards of other users.

Domain separation and Time Card

Domain separation is supported in Time Card. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can control several aspects of this separation, including which users can see and access data.

Support level: Basic

- Business logic: Ensure that data goes into the proper domain for the application’s service provider use cases.
- The application supports domain separation at run time. The domain separation includes separation from the user interface, cache keys, reporting, rollups, and aggregations.
- The owner of the instance must set up the application to function across multiple tenants.

Use case: When a service provider (SP) uses chat to respond to a tenant-customer’s message, the client must be able to see the SP's response.

To learn more, see Application support for domain separation.

Tools for driving tasks

There are several tools available to drive tasks to completion.

These tools can be run on any table which extends Task.

- Approvals
  Approvals can be generated to a list of Approvers, either manually or automatically, according to Approval Rules. Approvals can be incorporated into workflows or can stand alone. For more information, see Process approvals.
  Approvals can be used on tables that do not extend Task.
- Assignments
  Assignment rules can automatically assign tasks to users or groups, ensuring that the most appropriate team members handle the tasks. For more information, see Defining Assignment Rules.
- Service levels
  Service level agreements can track the amount of time that a task has been open, to ensure that tasks are completed within an allotted time.
- Inactivity monitors
  Inactivity monitors ensure that tasks do not fall by the wayside by notifying users when tasks have been untouched for a predefined period of time. For more information, see Setting Inactivity Monitors.
- **Workflow**

  An administrator can specify a specific workflow process to apply to tasks that meet certain conditions. After a task is created that meets the conditions, the workflow applies an automated process to the task. The process is defined in the graphical Workflow Editor.

  ![Graphical Workflow Editor](image)

  **Graphical Workflow Editor**

  As the process takes place, it updates any field designated as a workflow field.

  ![Workflow field](image)

  **Workflow field**

  Workflows are not specific to the tasks, but there are task-specific Workflow Activities (such as Task Activities and Approval Activities). For more information, see Workflow Overview.
Many to many task relations

By default, tasks can be related to each other using a parent/child relationship, such as a Problem with a group of child Incidents or a Catalog Request with a group of child Catalog Tasks.

However, it may prove useful to record exactly the nature of the relationship between the task records. When activated, the Many to Many Task Relations plugin allows administrators to define relationships between different tasks.

Request many to many task relations

The Many to Many Task Relations plugin is included with several plugins. You can request activation of the plugin by itself.

Role required: admin

- Planned Task
- Field Service Management
- Project Management
- Governance, Risk, and Compliance

1. Navigate to System Applications > All Available Applications > All.
2. On the All Applications page, click **Request Plugin** to open the Request form on HI.
3. On Now Support, select the redirect link to access the Now Support Service Portal Service Catalog.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Instance</td>
<td>Instance on which to activate the plugin.</td>
</tr>
<tr>
<td>Plugin Name</td>
<td>Name of the plugin to activate.</td>
</tr>
<tr>
<td>Specify the date and time you</td>
<td>The date and time must be at least two business days from the current time.</td>
</tr>
<tr>
<td>would like this plugin to be</td>
<td></td>
</tr>
<tr>
<td>enabled</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Plugins are activated in two batches, once in the morning and once in the evening, on every business day in the US Pacific time zone. If the plugin must be activated at a specific time, enter the request in the **Reason/Comments** field.

4. On the form, fill in the fields.

**Activate Plugin request form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reason/Comments</td>
<td>Information that would be helpful for the ServiceNow personnel who are</td>
</tr>
<tr>
<td></td>
<td>activating the plugin. For example, if you need the plugin activated at a</td>
</tr>
<tr>
<td></td>
<td>specific time instead of during one of the default activation windows,</td>
</tr>
<tr>
<td></td>
<td>specify that in the comments.</td>
</tr>
</tbody>
</table>

5. Click **Submit**.

**Plugin manifest**

When the plugin is activated, the Task Relationships application is available with certain modules.

When the plugin is activated, the **Task Relationships** application is available with the following modules:
Task relationships

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge Relation Types</td>
<td>Contains the definitions for the possible types of relationships between knowledge articles and tasks.</td>
</tr>
<tr>
<td>Knowledge Relationships</td>
<td>Displays all the defined relationships between existing tasks and knowledge articles.</td>
</tr>
<tr>
<td>Relationship Types</td>
<td>Contains the definitions for the possible types of relationships between tasks.</td>
</tr>
<tr>
<td>Relationships</td>
<td>Contains all the defined relationships between existing tasks.</td>
</tr>
</tbody>
</table>

The following Relation Types are available by default:

- Knowledge Relation Types
  - Solution is documented in::Documenting solution for

- Relationship Types
  - Caused by::Causes
  - Contains::Task of
  - Documenting Solution for::Solution is documented in
  - Investigated by::Investigates
  - Permanent correction for::Permanently corrected by
  - Related to::Related to
  - Requesting::Requested by
  - Solved by::Solves

Define a relationship type

Create type codes that define the relationship between parent and child tasks.

The Many to Many Task Relations plugin must first be activated. To learn more, see Request many to many task relations.

1. Navigate to Task Relationships > Relation Types and click New.
2. Populate the Parent Descriptor and Child Descriptor fields with a short description of the relationship between the two tasks, such as a parent descriptor of Caused By and a child descriptor of Causes.
3. Right-click the form header bar and select Save. The Name field automatically populates with the Parent and Child descriptors.

Define a task relationship allowed from the task relationship type record

It is possible to define Task Relationships Allowed from the Task Relationship Type record.

1. Scroll down to the related list and click New.
2. Populate the parent and child tables to define which tables are able to accept the relationship.
3. If desired, it is possible to define scripts to run in the Parent and Child script fields. These scripts are run when a parent or child record is run to automatically generate the other task (child or parent). These scripts use the current value of the new record, as opposed to the source record which triggered the script.

Modify the displayed field

The list view of the Reference Lookup defines the fields displayed in the Task Relations field and editing interface. To modify the displayed fields:

1. Navigate to a form that has a reference to the table whose display values you would like to modify within Task Relations field.
2. Click the magnifying glass to display the Reference Lookup list view.
3. Right-click the list header and select Configure > List Layout. The selected List layout is used as the display value for records within the Task Relations field.

Mark as Solution button

This button gets added to the KB popup view and is displayed when you search the knowledge base from a task record. Clicking the button creates a record in the Task / KB Relationships [task_rel_kb] table to associate the KB article with a task. You can disable this button by marking the active field false on the 'solution_button' UI macro.

Define task relationships with UI actions

Once the task relationships are defined, it is possible to use UI Actions to define the task relationship as a new task is being created from an old task.
Below are a few examples.

**Warning:** These examples may not work on all instances. They are provided as illustrative examples.

### UI Actions examples

#### Cause an incident

This UI Action allows the change management team to log an incident directly from the change request and records that the change caused the incident.

Create a UI Action on the Change Request [change_request] table and place the following into the script:

```javascript
var inccaus = new GlideRecord("incident");
inccaus.short_description= current.short_description;
inccaus.comments= current.comments.getHTMLValue();
// inccaus.parent = current.sys_id;
inccaus.insert();
CauIncident();

gs.addInfoMessage("Incident " + inccaus.number+" created");
action.setRedirectURL(current);
action.setReturnURL(inccaus);

function CauIncident(){
  var m2m = new GlideRecord('task_rel_task');
m2m.initialize();
m2m.child= current.sys_id;
m2m.parent= inccaus.sys_id;
m2m.type.setDisplayValue("Caused by::Causes");
m2m.insert();}
```

#### Cause a problem

This UI Action allows the change management team to record a problem from a change request and record that the change caused the problem.

Create a UI Action on the Change Request [change_request] table and paste the following script:

```javascript
var probcaus = new GlideRecord("problem");
probcaus.short_description= current.short_description;
probcaus.comments= current.comments.getHTMLValue();
// probcaus.parent = current.sys_id;
probcaus.insert();
CauProblem();

gs.addInfoMessage("Problem " + probcaus.number+" created");
action.setRedirectURL(current);
action.setReturnURL(probcaus);

function CauProblem(){
  var m2m = new GlideRecord('task_rel_task');
m2m.initialize();
m2m.child= current.sys_id;
m2m.parent= probcaus.sys_id;
m2m.type.setDisplayValue("Caused by::Causes");
m2m.insert();}
```
Fix a problem

This UI Action allows a change request to be generated from a problem, recording that the change fixes the problem.

Create a UI Action on the Problem [problem] table, and paste the following code:

```javascript
var fixchg = new GlideRecord("change_request");
fixchg.short_description = current.short_description;
fixchg.comments = current.comments.getHTMLValue();
// fixchg.parent = current.sys_id;
fixchg.insert();
FixChange();
gs.addInfoMessage("Change " + fixchg.number + " created");
action.setRedirectURL(current);
action.setReturnURL(fixchg);

function FixChange(){
var m2m = new GlideRecord('task_rel_task');
m2m.initialize();
m2m.child = current.sys_id;
m2m.parent = fixchg.sys_id;
m2m.type.setDisplayValue("Fixes::Fixed by");
m2m.insert();}
```

Data dictionary tables

The system defines data dictionary, data modeling, and entity relationship information in multiple tables.

- Tables [sys_db_object]: Contains a record for each table.
- Dictionary Entries [sys_dictionary]: Contains additional details for each table and the definition for every column on each table. Each row represents either a column on a table or a table.
- Field Labels [sys_documentation]: Contains the human-readable labels and language information.

Tables

The Tables [sys_db_object] table contains a record for each table in the database.

Access the Tables list by navigating to System Definition > Tables. Administrators can create a custom table, add or modify columns in a searchable and sortable embedded list, and define the auto-number format.

The following image shows a list of the tables that extend the Task table.
Tables

Dictionary Entries

The Dictionary Entries [sys_dictionary] table, also called the **System Dictionary**, defines every table and field in the system. It contains information about data type, character limit, default value, dependency, and other attributes of a field.

Access the system dictionary in one of these ways:

- To see the system dictionary list view, navigate to **System Definition > Dictionary**.
- To view particular dictionary definition, right-click the list header, form header, or field label, and select **Configure Dictionary**.

The following image shows a filtered list of dictionary entries for the Incident table and the Task table, which it extends.
Dictionary Inc Task

Field Labels

The Field Labels [sys_documentation] table, also called the Language File, contains information about the labels and hints for each table and column in the system.

Access the language file in one of these ways:

- To see the list view, navigate to System Definition > Language File.
- To see the field label for a particular field, right-click the field label on the form.

The following image shows the language file filtered to display only labels on the Incident table.
The system dictionary is a table, called Dictionary Entry [sys_dictionary], that contains details for each table and the definition for every column on each table in an instance.

Each row in the system dictionary represents either a table or a column in one of the tables. The system dictionary provides options for administrators to modify tables and fields, which in turn define lists and forms.

Use caution when changing system dictionary records because changes can have a high impact on functionality. In particular, changes to dictionary entries for system tables, which are tables that begin with sys_, can create system-wide issues such as the inability to use update sets.

Dictionary changes are difficult to reverse. Also, dictionary changes automatically apply to all extended tables unless a dictionary override is defined. Be sure that changes are well-tested before applying them to a production instance.

**Creation options**

When you create a field from the system dictionary, it is automatically added at the end of the first section of the default form view.

In most cases, use the following interfaces rather than creating entries directly on the system dictionary:

- To create tables and fields, use the Tables module.

```
<table>
<thead>
<tr>
<th>Table</th>
<th>Element</th>
<th>Language</th>
<th>Label</th>
<th>Plural</th>
<th>Hint</th>
<th>Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>incident</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Business duration</td>
<td>2011-08-19 15:35:37</td>
</tr>
<tr>
<td>incident</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Business resolve time</td>
<td>2021-01-24 19:46:30</td>
</tr>
<tr>
<td>incident</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Caller</td>
<td>Person who reported or is affected by th...</td>
</tr>
<tr>
<td>incident</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Category</td>
<td>Categories</td>
</tr>
<tr>
<td>incident</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Caused by Change</td>
<td>Caused by Changes</td>
</tr>
</tbody>
</table>
```
To create fields, configure the table form.

**Dictionary overrides**

Dictionary overrides provide the ability to define a field on an extended table differently from the field on the parent table.

For example, for a field on the Task [task] table, a dictionary override can change the default value on the Incident [incident] table without affecting the default value on Task [task] or on Change [change].

Administrators can override these aspects of a field:

- Reference qualifiers
- Dictionary attributes
- Default values
- Calculations
- Field dependencies
- Default column display values
- Mandatory and read-only status

**Define a dictionary override**

Use a dictionary override to allow a field in a child table to have a different value or behavior than the same field in a parent table. For example, a dictionary override changes the default value of the priority field from 4 in the parent table to 5 in the Incident table.

Dictionary overrides are only available for tables that support table extension. You can only add dictionary overrides on tables that are in the same scope as the parent table.

1. Navigate to **System Definition > Dictionary**.
2. Open the record for the field.
3. In the **Dictionary Overrides** related list, click **New**.
4. Fill in the fields on the form, as appropriate (see table).

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>The application scope to which the record belongs.</td>
</tr>
<tr>
<td>Base table</td>
<td>The parent table containing the field to override.</td>
</tr>
<tr>
<td>Table</td>
<td>Select the extended table to which the dictionary override applies.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The list shows only tables and database views that are in the same scope as the dictionary override.</td>
</tr>
<tr>
<td>Override reference qualifier</td>
<td>Select the check box to display the Reference qualifier field, which overrides the reference qualifier for the field on the extended table.</td>
</tr>
<tr>
<td>Override dependent</td>
<td>Select the check box to display the Dependent field, which overrides the field on which the current field depends.</td>
</tr>
<tr>
<td>Override attributes</td>
<td>Select the check box to display the Attributes field, which overrides the dictionary attributes for the field on the extended table.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Note:</td>
<td>Any attributes defined on the base table are ignored. If there are attributes on the base table that should still apply to the extended table, make sure to include them in this field.</td>
</tr>
<tr>
<td>Override default value</td>
<td>Select the check box to display the Default Value field, which overrides the default value for the field on the extended table.</td>
</tr>
<tr>
<td>Override calculation</td>
<td>Select the check box to display the Calculation field, which overrides the calculation of the value for the field on the extended table.</td>
</tr>
<tr>
<td>Override mandatory</td>
<td>Select the check box to display the Mandatory field, which overrides whether the field on the extended table must contain a value to save a record.</td>
</tr>
<tr>
<td>Override read only</td>
<td>Select the check box to display the Read only field, which overrides whether a user can change the field value on the extended table.</td>
</tr>
<tr>
<td>Override display value</td>
<td>Select the check box to use this field as the display value on the extended table.</td>
</tr>
<tr>
<td></td>
<td>For example, the Story [rm_story] table uses the short description as the display value in reference fields instead of the number, as defined in the Task [task] table.</td>
</tr>
</tbody>
</table>

5. Click Submit.

**Modify dictionary entries**

You can modify dictionary entries by configuring a field on a form or from the Dictionary module.

1. Do one of the following steps:
   - Navigate to a field on a form, right-click the field, and select Configure Dictionary or Show <field name>. The system dictionary entry for the field opens.
   - Navigate to System Definition > Dictionary, and click an entry for a field or table. Entries for tables have Type set to Collection.

2. Update the dictionary entry fields.

3. Click Update.

**Dictionary entry form**

The Dictionary Entry form was redesigned to provide an Advanced view and additional fields. You might need to configure the form to see all fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note:</td>
<td>This list shows only the tables that meet the scope protections for adding fields.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Defines the field type of the column or, if the <strong>Type</strong> is <strong>Collection</strong>, indicates that the dictionary entry represents the table. For more information, see Introduction to Fields. You can change the type of a field. To preserve existing data, only change between logical types that map to the same physical type on the database. For example, Choice and String.</td>
</tr>
<tr>
<td><strong>Active</strong></td>
<td>Enables or disables the field. When this check box is cleared, the field is not used by the system.</td>
</tr>
<tr>
<td><strong>Function field</strong></td>
<td>If selected, creates a field that displays the results of a database function, such as a mathematical operation, field length computation, or day of the week calculation. Once the new function record is saved, you cannot clear the check box to make the field a regular field.</td>
</tr>
<tr>
<td><strong>Read only</strong></td>
<td>Determines whether users can change the field value. When this check box is selected, users cannot change the value. The system calculates and displays the data for the field. <strong>Note:</strong> You can override this option for extended tables.</td>
</tr>
<tr>
<td><strong>Audit</strong></td>
<td>Enables or disables auditing for a table. Turning on Auditing (History) for a Table. <strong>Note:</strong> This option only applies to tables.</td>
</tr>
<tr>
<td><strong>Text index</strong></td>
<td>Determines whether searches index the text in a table. <strong>Note:</strong> This option only applies to tables. To exclude fields from indexing, see Remove an Index for a Specific Field.</td>
</tr>
<tr>
<td><strong>Column label</strong></td>
<td>Defines a unique label for the column. The label appears on list headers and form fields for the column. • Updating the <strong>Column label</strong> field also updates the label in the language file (for the current language). • When you create a new column, the column name is populated automatically based on the label, which is prefixed with <strong>u_</strong> to indicate that it is custom. For example, if you enter <strong>Activity Description</strong> as the column label, the column name defaults to <strong>u_activity_description</strong>.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Column name</td>
<td>Defines the field name of the column. When you create a new field, this name is populated automatically based on the label and a prefix as follows:</td>
</tr>
<tr>
<td></td>
<td>• For a field on a table in a different scope, the name is prefixed with the scope to indicate that it is custom and not part of that application.</td>
</tr>
<tr>
<td></td>
<td>• For a field on a table in the same scoped application, the name does not have a prefix, which indicates that it is part of the application.</td>
</tr>
<tr>
<td></td>
<td>• For a field in a global application, the name is prefixed with u_ to indicate that it is custom.</td>
</tr>
<tr>
<td></td>
<td>You cannot modify the prefix; however, you can modify the rest of the name. The name can contain only lowercase, alphanumeric ASCII characters and underscores (_). You cannot change the name of an existing dictionary record.</td>
</tr>
</tbody>
</table>

**Note:** You cannot enter consecutive (double) underscores in a column name. For example, if you enter my sample name as the column name, it is automatically changed to my_sample_name when you save the dictionary entry.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max length</td>
<td>Provides a logical limit for the size of string fields to determine how the system displays them in the user interface and how to map them to physical database data types. String fields with a length under 255 characters appear as a single-line text fields. String fields with a length over 254 characters appear as a multi-line text box. The system maps the field length to the closest physical data type available on the database. Sometimes, this results in more available length than originally specified. For example, entering a length of 50 maps to the closest physical data type of VARCHAR(100), which provides up to a 100 character limit or double the requested field length. Likewise, entering a length of 1000 maps to the closest physical data type of MEDIUMTEXT, which provides up to a 4000 character limit or four times the requested field length.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td></td>
<td>• You can only change this value for a <strong>String</strong> field. Changes for any other type of field are ignored.</td>
</tr>
<tr>
<td></td>
<td>• Users on an Oracle instance cannot increase the maximum length of a string field to anything greater than 4000 through the application UI as this requires the CLOB datatype in Oracle. To increase beyond this size, log an incident with technical support to request the change.</td>
</tr>
<tr>
<td></td>
<td>• To prevent data from being lost, only decrease the length of a string field when you are developing a new application and not when a field contains data. A warning appears if a change to a custom field results in data loss. For a base system field, you cannot make a change that results in data loss.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mandatory</th>
<th>Determines whether this field must contain a value to save a record. For more information, see <a href="#">Creating Mandatory Fields</a>.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Note:</strong> You can override this option for extended tables.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Display</td>
<td>Indicates that this field is the display value for reference fields. Set this to true for the one field whose value you want to use as the text displayed in links to this table on lists and forms. By default, the <strong>Number</strong> field is the display value for all task tables.</td>
</tr>
<tr>
<td>Function definition</td>
<td>Defines the function that the field performs.</td>
</tr>
<tr>
<td>Attributes [Advanced view]</td>
<td>Alters the behavior of a field or functionality that depends on the field. For more information, see Dictionary Attributes. Attributes can be overridden for extended tables with dictionary overrides. You can also configure attributes for this dictionary entry through the Attributes related list.</td>
</tr>
<tr>
<td>Default Value</td>
<td></td>
</tr>
<tr>
<td>Use dynamic default [Advanced view]</td>
<td>Allows you to specify a default value that is generated dynamically based on a dynamic filter.</td>
</tr>
<tr>
<td>Dynamic filter value [Advanced view]</td>
<td>Specifies the dynamic filter that determines the default value if the <strong>Use dynamic default</strong> option is selected.</td>
</tr>
<tr>
<td>Default value</td>
<td>Specifies the default value of the field for any new record. Ensure that this value uses the correct field type. For example, an integer field uses a default value of 2 but cannot use a default value of two. These values can be overridden with dictionary overrides.</td>
</tr>
</tbody>
</table>

**Note:**
- This option does not control whether a list or form displays this field as part of the layout. Instead, see List Configuration and Personalizing Forms.
- The display value becomes part of the form title when viewing an individual record from a table.
- You can set a different display value on an extended table than the display value on a parent table by using a dictionary override.

Note: Function parameters support dot walking. See Dot-walking to data in related tables.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reference</td>
<td>Makes the field into a reference field. If you enter a name that does not match an existing table, a new table is created when you save your changes to the dictionary record. If the current table has a module in the application navigator, a module for the new table is automatically created in the same application menu.</td>
</tr>
</tbody>
</table>
| Use reference qualifier [Advanced view] | Specifies the type of qualifier to use:  
• Simple: A set of choice lists where you can specify a reference qualifier condition.  
• Dynamic: A dynamic filter that you can use to build the qualifier.  
• Advanced: A static encoded query string or JavaScript code that you can use to build the qualifier. |
| Reference qual condition             | Specifies a condition when the reference qualifier runs if the Simple qualifier type is selected.                                                                                                           |
| Dynamic ref qual [Advanced view]     | Specifies the dynamic filter that determines the reference qualifier when the Dynamic qualifier type is selected.                                                                                          |
| Reference qual [Advanced view]       | Filters the records available for a reference field if the Advanced qualifier type is selected. Reference qualifiers can be overridden with dictionary overrides.                                               |
| Reference key [Advanced view]        | Identifies a field other than sys_id to use as the unique identifier for reference fields.                                                                                                                |
| Reference cascade rule [Advanced view] | Defines what happens to a record if the record it references is deleted. Select one of the following options:  
• Clear: Clears the references (default).  
• Delete: Deletes all referencing records.  
• Restrict: Prevents record deletion if there is a referencing record.  
• None: Does not change referencing records. |
<p>| Reference floats [Advanced view]      | Enables the Edit button on related lists for one-to-many relationships.                                                                                                                                 |
| Dynamic creation [Advanced view]     | For reference fields, determines whether entering a value that does not match an existing record creates a record on the referenced table. If selected, use the Dynamic creation script field to define how to create the record. |
| Dynamic creation script [Advanced view] | When the Dynamic creation field is selected, allows you to enter a script for creating a record on the referenced table.                                                                                     |
| Dependent Field                      | Specifies a field on which the current field depends. For more information, see Configuring Dependent Fields.                                                                                             |
| Dependent on field [Advanced view]   | Note: You can override this value for extended tables.                                                                                                                                                     |
| Choice List Specification            |                                                                                                                                                                                                           |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Choice                   | Allows users to see a list of suggested values in one of the following ways:  
  - List menu without -- None --  
  - List menu with -- None --  
  - Suggestion  
  
  If a choice is used, either define a choice list or use the fields Choice table and Choice field to copy choices from another field elsewhere in the dictionary.                                                                                                                                                                                                                                                                                                                                                      |
| Choice table [Advanced view] | Populates the field choices with the same values as another choice field. If the Choice field is set to anything besides None, select a table to draw choice values from. The field Choice field must also be populated.  
  
  For example, if Choice table is set to the Incident [incident] table, this field has the same choice list as one of the choice fields on Incident. Choice field (see below) determines which field.                                                                                                                                                                                                                                                                                                                                                                                                 |
| Choice field [Advanced view] | Populates the field choices with the same values as another choice field. If the Choice field is set to anything besides None, select a field from the table you selected for Choice table. For example, if the Choice table field is set to the Incident [incident] table, and Choice Field is set to Priority, this field has the same choices as the Priority field on Incident, even if those choices change.  
  
  Note: This field must be a choice field.                                                                                                                                                                                                                                                                                                                                                                                                       |
| Calculated Value         | Determines whether the value of the field is calculated from other values. If selected, use the Calculation field to define how the calculation is performed. When sorting or grouping by a calculated field, the sort order is based on the field value from the last time the field was updated, not the last time the field was displayed.  
  
  Note: In relation to business rules, calculated fields are populated first before any business rule, even a before business rule, is run. Calculated fields are then populated again if necessary after any before business rules run.                                                                                                                                                                                                                                                                                                                                 |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
<td>Identifies the table that the current table extends. Tables that do not extend other tables specify their own name in this field. For more information, see .</td>
</tr>
<tr>
<td>Defaultsort</td>
<td>Obsolete.</td>
</tr>
<tr>
<td>Size class</td>
<td>Determines whether the platform handles this table as a large table by reducing the amount of memory stored for each row during queries. There is a scheduled job which runs and sets the value of this field.</td>
</tr>
<tr>
<td>Spell check</td>
<td>Enables or disables spell check on the field. For more information, see Adding Spell Check to a Field.</td>
</tr>
<tr>
<td>Unique</td>
<td>Requires the field value to be unique.</td>
</tr>
<tr>
<td>UI action</td>
<td>Changes the form view to the default or advanced view. The fields change based on the view. If you are using the default view, you must write a script to accomplish the same tasks that advanced view fields provided.</td>
</tr>
<tr>
<td>Related Lists</td>
<td></td>
</tr>
<tr>
<td>Access Controls</td>
<td>Provides access to the access controls that permit or limit access to the data in the table.</td>
</tr>
<tr>
<td>Choices</td>
<td>Provides access to the options in the choice list field you are editing.</td>
</tr>
<tr>
<td>Dictionary overrides</td>
<td>Provides access to the dictionary overrides for this field.</td>
</tr>
<tr>
<td>Attributes</td>
<td>Provides access to the dictionary attributes for this entry.</td>
</tr>
<tr>
<td>Labels</td>
<td>Provides access to the labels used for the table or field you are editing.</td>
</tr>
</tbody>
</table>

**Dictionary attributes**

Dictionary attributes alter the behavior of the table or element that the dictionary record describes. Administrators can add or modify dictionary attributes.

**Adding an attribute**

To add an attribute to a table or field, navigate to the System Dictionary record for the Dictionary entry, and add the attribute to the Attributes field. Attributes are comma-separated; if attributes exist on a dictionary record, add a comma, with no spaces, before adding an attribute.

For an attribute that accepts true/false values:

- To specify a value of true, you can either enter attribute or attribute=true.
• To specify a value of false, you can either ensure that the attribute does not appear or enter `attribute=false`. To maintain values during upgrades, do not remove an attribute that is on a table by default.

**Maintaining attribute values for upgrades**

If you remove an attribute that is part of the base system, it is automatically restored during an upgrade. To prevent upgrades from changing the desired behavior of your system, leave the attribute on the table or field, but set its value as desired.

For example, if a field has the attribute `knowledge_search=true` by default, do not remove the attribute to set it to false; rather set it to `knowledge_search=false`.

**Available dictionary attributes**

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
<th>Target Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow_null</td>
<td>true/false</td>
<td>field_name field</td>
<td>If present or true, enables you to enter None as the field</td>
</tr>
<tr>
<td>allow_public</td>
<td>true/false</td>
<td>table_name field</td>
<td>If true, the table name field displays tables from all scopes instead of only the current scope.</td>
</tr>
<tr>
<td>allow_references</td>
<td>true/false</td>
<td>field_name field</td>
<td>If true, a tree is displayed to select from that includes reference fields so you can dot-walk.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td><strong>Value</strong></td>
<td><strong>Target Element</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>----------</td>
<td>-----------</td>
<td>--------------------</td>
<td>-----------------</td>
</tr>
</tbody>
</table>
| approval_user | name of field containing the users for the approval type this field represents | integer field | Table fields are used to perform lookups using a matcher. You specify approvals as table fields that have an attribute of `approval_user=<field_name>`, where `<field_name>` indicates the field in the table that contains the users for this approval type.  
- Fields with this attribute contain an integer value that indicates the sequence for the approvals.  
- All approval fields with the same sequence number indicate that multiple approvals are required before continuing.  
- Approvals are requested in the order of the sequence numbers. For example, all approvals with sequence number 100 must be approved before approvals with sequence number 200 are requested. |
<p>| attachment_index | true/false | any table | If true, attachments on the table are indexed for search purposes. To learn more, see Index attachments on a table. |
| barcode | true/false | string field | Enables a string field in the ServiceNow Classic app to access a camera on a mobile device to scan and process a bar code. To learn more, see Using the ServiceNow Classic mobile app. |
| base_table | name of base table type | table_name field | A table_name field enables you to select any table derived from the table specified by this attribute. By default, the base table itself is also included in the list (but see <code>skip_root</code> to turn off this behavior). |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
<th>Target Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>calendar_elements</td>
<td>list of field names, separated by semicolons (&quot;;&quot;)</td>
<td>any calendar event table</td>
<td>Specifies a list of fields used when constructing the description of a calendar event. If not specified, the usual display name plus short description are used. The <strong>calendar_elements</strong> attribute does not support derived (dot-walked) fields.</td>
</tr>
<tr>
<td>collection_interval</td>
<td>interval specified as &quot;HH:MM:SS&quot; (like &quot;01:02:30&quot; for one hour, two minutes, and 30 seconds)</td>
<td>collection field</td>
<td>Specifies the interval of metrics collection.</td>
</tr>
<tr>
<td>close_states</td>
<td>inactive state integer values</td>
<td>task state field</td>
<td>Used by the TaskStateUtil API to identify the list inactive state values delimited by semicolons (;)</td>
</tr>
<tr>
<td>critical</td>
<td>true/false</td>
<td>any field in the apm_application table</td>
<td>Defines fields that are critical information about an application, which enables tracking the entry of critical information.</td>
</tr>
<tr>
<td>current_location</td>
<td>true/false</td>
<td>string field</td>
<td>Enables a string field in the Using the ServiceNow Classic mobile app to access the GPS location of a mobile device.</td>
</tr>
<tr>
<td>disable_execute_now</td>
<td>true/false</td>
<td>any table derived from sys_auto</td>
<td>If present or true, disables the usual <strong>Execute Now</strong> button. Now Platform applications that use schedules (such as Discovery) use this attribute to substitute their own more appropriate action.</td>
</tr>
<tr>
<td>default_rows</td>
<td>integer value</td>
<td>multitext fields</td>
<td>Sets the default number of rows in a multitext field.</td>
</tr>
<tr>
<td>default_close_state</td>
<td>state integer value</td>
<td>task state field</td>
<td>Used by the TaskStateUtil API to identify the default close state value for a task table</td>
</tr>
<tr>
<td>default_work_state</td>
<td>state integer value</td>
<td>task state field</td>
<td>Used by the TaskStateUtil API to identify the default working state value for a task table</td>
</tr>
<tr>
<td>Name</td>
<td>Value</td>
<td>Target Element</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------</td>
<td>----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>detail_row</td>
<td>name of field to display in detail row</td>
<td>any table</td>
<td>Displays the value of the specified field as a detail row for each record in the list view. UI15 is required to use this attribute.</td>
</tr>
<tr>
<td>document_viewer_audit</td>
<td>view, download, or all</td>
<td>any table</td>
<td>When the Document Viewer is enabled, this attribute keeps a record of user actions performed on attachments. The values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• <strong>view</strong>: Enables an audit when users view an attachment</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• <strong>download</strong>: Supplies audit information for only downloaded attachments</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• <strong>all</strong>: Shows audit information when attachments are viewed and downloaded</td>
</tr>
<tr>
<td>email_client</td>
<td>true/false</td>
<td>any table</td>
<td>If present or true, causes an icon (an envelope) to appear in the more options menu in the form header. If you click it, a pop-up email client appears.</td>
</tr>
<tr>
<td>exclude_auto_recovery</td>
<td>true/false</td>
<td>any table</td>
<td>Disables automatic recovery of draft records for this table and its extensions.</td>
</tr>
<tr>
<td>extensions_only</td>
<td>true/false</td>
<td>any table</td>
<td>Table should only have records in tables that extend it. For example, the Task table has this attribute because you would create incident, problem, change records, and not task records.</td>
</tr>
<tr>
<td>Name</td>
<td>Value</td>
<td>Target Element</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------</td>
<td>----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>field_list_selector</td>
<td>true/false</td>
<td>any glide_list</td>
<td>Enables the user to select a field from the dependent table (or current if dependent is not specified). Some workflow activities use this attribute.</td>
</tr>
<tr>
<td>field_decorations</td>
<td>UI Macro name list, separated by semicolons (;;)</td>
<td>most fields (except list and multiline text fields)</td>
<td>Similar to ref_contributions, causes the named UI macro to be invoked when the field is rendered on a form.</td>
</tr>
</tbody>
</table>
| format                   | format name                                      | any numeric field | Specifies a named format to use instead of the standard numeric formatting. Options are:  
  - **glide_duration**: Formats a time specified in milliseconds as $ddd hh:mm:ss$.  
  - **none**: Disables automatic number formatting (for example, changes 2,500–2500). |
<p>| glide.db.oracle.ps.query | true/false                                      | any table       | If present and false, prevents the use of Oracle prepared queries on the table.                                                            |
| global_visibility        | true/false                                      | any table with a sys_domain column | If present or true, makes this table visible globally even if there are domain restrictions (that is, the sys_domain field has a value). |
| hasLabels                | true/false                                      | any table       | If present or true, marks this table as the target of a label at some point. You can manually set this attribute, but it is normally set automatically whenever a label is generated. When true, the label engine runs on any change to the table, updating the labels as needed. |
| hasListeners             | true/false                                      | any table       | If present or true, marks this table as available for listeners to get events (insert, update, delete) on.                                      |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
<th>Target Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hasWorkflow</td>
<td>true/false</td>
<td>any table</td>
<td>Instructs the workflow engine to listen for changes to the table, firing events to a workflow when a record associated with a particular workflow has changed.</td>
</tr>
<tr>
<td>html_sanitize</td>
<td>true/false</td>
<td>any HTML or translated HTML field</td>
<td>If present or true, enables HTML sanitization for the selected HTML or Translated HTML field. By default, performs HTML Sanitization on all HTML and Translated HTML fields. Set this attribute to false to disable sanitization.</td>
</tr>
<tr>
<td>html_sanitize_config</td>
<td>name of custom sanitizer configuration file</td>
<td>any HTML or translated HTML field</td>
<td>If present, performs sanitization using the specified configuration file instead of the default platform sanitizer. For example, the Embedded Help [sys_embedded_help_content] table uses a specified file (EmbeddedHelpSanitizerConfig) for the help Content field.</td>
</tr>
<tr>
<td>icons</td>
<td>name of JavaScript class</td>
<td>any workflow field</td>
<td>Specifies a JavaScript class that produces workflow icons.</td>
</tr>
<tr>
<td>image</td>
<td>relative path of image file</td>
<td>any table</td>
<td>Specifies an image file to use when a module or BSM map uses this table. This specification overrides the icons that would otherwise be used for the table.</td>
</tr>
<tr>
<td>include_container_types</td>
<td>true/false</td>
<td>any internal_type field</td>
<td>Causes the field to render with container (split) types as well other types.</td>
</tr>
<tr>
<td>isOrder</td>
<td>true/false</td>
<td>any field</td>
<td>Sets the field as the default field used for the sort order in lists. Overridden by the ORDERBY URL parameter, or the user's sort preferences.</td>
</tr>
<tr>
<td>iterativeDelete</td>
<td>true/false</td>
<td>any table</td>
<td>If present or true, forces all row deletes to execute iteratively. Otherwise, you can perform some deletes using a more efficient bulk method.</td>
</tr>
<tr>
<td>Name</td>
<td>Value</td>
<td>Target Element</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------</td>
<td>----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>json_view</td>
<td>true/false</td>
<td>any table</td>
<td>if a JSON object is associated with the field, places an icon next to a field that, when you click it, displays data interchange information.</td>
</tr>
<tr>
<td>knowledge_custom</td>
<td>name of JavaScript function</td>
<td>any field</td>
<td>Specifies a JavaScript function to implement a custom knowledge search (see knowledge_search).</td>
</tr>
<tr>
<td>knowledge_search</td>
<td>true/false</td>
<td>string fields</td>
<td>If present or true, causes a knowledge search icon (a small book) to appear next to the field. Clicking this icon launches a pop-up window for searching the knowledge base, unless a custom knowledge search function has been specified. To learn more, see knowledge_custom.</td>
</tr>
<tr>
<td>largeTable</td>
<td>true/false</td>
<td>any table</td>
<td>If present or true, marks this table as &quot;large&quot; to preventing table locking with specific MySQL database operations (adding/removing a column/index, compacting a table). Without this attribute (or the smallTable attribute), the glide.db.large.threshold property, or the default value of 5,000, determines whether a table is large.</td>
</tr>
<tr>
<td>listen</td>
<td>true/false</td>
<td>any field</td>
<td>If present or true, calls a JavaScript function named &lt;tableName&gt;_&lt;fieldName&gt;Listen, or globalListen if that function does not exist. It calls the function with arguments (tableName, fieldName, oldValue, newValue).</td>
</tr>
<tr>
<td>Name</td>
<td>Value</td>
<td>Target Element</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------</td>
<td>----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>live_feed</td>
<td>true/false</td>
<td>any field</td>
<td>If present or true, creates a toggle option on the activity formatter header for incidents, tasks, and problems. The toggle provides a choice between the <strong>Live Feed</strong> for that record (also known as a document feed) or the activity formatter fields already in use. To learn more, see Activity formatter for more details.</td>
</tr>
<tr>
<td>long_label</td>
<td>true/false</td>
<td>any reference field</td>
<td>Long or short labels refer to the label that appears for reference fields on a form. For example, if the reference field contains the caller’s email address, the long label would be Caller Email, while the short label would be Email. • Usually the placement of the reference field on the form makes it clear what the field represents. • It uses the global property <code>glide.short.labels</code> to specify the type of labels that appear for all reference fields on any form. • You can override the global property for any reference field by setting the <code>short_label=true</code> or <code>long_label=true</code> attribute in the dictionary for the reference field.</td>
</tr>
<tr>
<td>Name</td>
<td>Value</td>
<td>Target Element</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------</td>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>maintain_order</td>
<td>true/false</td>
<td>any glide_list</td>
<td>If present or true, the up/down arrow order buttons appear to the right of the list of selected items.</td>
</tr>
<tr>
<td>mode_toggler</td>
<td>true/false</td>
<td>any composite_name</td>
<td>If present or true, causes a name mode toggle icon (a small right-pointing triangle) to appear to the right of the label. Clicking this icon causes the field's rendering to change from a text field accepting <code>&lt;tablename&gt;.&lt;fieldname&gt;</code> to a pair of reference choice boxes (one for the table, the other for the field). The latter is the default.</td>
</tr>
<tr>
<td>model_class</td>
<td>binary Java class name</td>
<td>any field of type glide_var</td>
<td>Specifies a model variable within Java code. The model must have a class that implements the IVariablesModel interface.</td>
</tr>
<tr>
<td>model_field</td>
<td>see description</td>
<td>any field of type glide_var</td>
<td>Identifies a reference field in the record that has the model defined for it. For example, a workflow activity is associated with an activity definition. The activity definition has a related list of questions that make up the model for that activity definition. By using the activity_definition as the model_field for the activity, it builds the workflow activity model by reading the questions that are defined for the referenced activity definition.</td>
</tr>
<tr>
<td>nibble_size</td>
<td>positive integer</td>
<td>any table affected by the table cleaner.</td>
<td>Specifies the maximum number of records the table cleaner can delete in a single operation. The default value for this attribute is 250.</td>
</tr>
<tr>
<td>Name</td>
<td>Value</td>
<td>Target Element</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>nibble_sleep</td>
<td>true/false</td>
<td>any table affected by the table cleaner.</td>
<td>If false, causes the table cleaner to perform cleanup operations without a pause between each operation.</td>
</tr>
<tr>
<td>no_add_me</td>
<td>true/false</td>
<td>any table</td>
<td>If present or true, hides display of the Add Me icon that appears next to certain fields, such as the <strong>Watch List</strong> field.</td>
</tr>
<tr>
<td>no_attachment</td>
<td>true/false</td>
<td>any table</td>
<td>If present or true, prevents the attachment icon (a paperclip) from appearing on the form header.</td>
</tr>
<tr>
<td>no_attachments</td>
<td>true/false</td>
<td>any table</td>
<td>If present or true, attachments are not checked for and deleted when a record from this table is deleted. Meant for high-activity tables that never have attachments.</td>
</tr>
<tr>
<td>no_audit</td>
<td>true/false</td>
<td>any table</td>
<td>If present or true, this field is not audited, even if the table is being audited.</td>
</tr>
<tr>
<td>no_audit_delete</td>
<td>true/false</td>
<td>any table</td>
<td>If present or true, a sys_audit_delete record is never created when you delete a record from this table. Meant for high-activity tables that never need sys_audit_delete information.</td>
</tr>
<tr>
<td>no_auto_map</td>
<td>true/false</td>
<td>any table</td>
<td>If true, this field is not mapped during an import set. Primarily used for LDAP imports.</td>
</tr>
<tr>
<td>no_email</td>
<td>true/false</td>
<td>any glide_list field referencing sys_user</td>
<td>If present or true, the email box is removed from the glide_list field like the <strong>Watch list</strong> field.</td>
</tr>
<tr>
<td>no_multiple</td>
<td>true/false</td>
<td>any glide_list field</td>
<td>Hides the select multiple icons.</td>
</tr>
<tr>
<td>Name</td>
<td>Value</td>
<td>Target Element</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------</td>
<td>----------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>no_optimize</td>
<td>true/false</td>
<td>any table</td>
<td>If present or true, prevents the MySQL table compaction operation from running on the specified table. The table compaction operation normally runs after the table cleaner deletes at least 50% of the data in the specified table.</td>
</tr>
<tr>
<td>no_separation</td>
<td>true/false</td>
<td>any table</td>
<td>If present or true, marks this table as not participating in domain separation. To learn more, see Domain separation for service providers.</td>
</tr>
<tr>
<td>no_text_index</td>
<td>true/false</td>
<td>any field</td>
<td>If a table is text indexed, the no_text_index field attribute prevents this field or child table from being included in the text index.</td>
</tr>
<tr>
<td>no_truncate</td>
<td>true/false</td>
<td>any string field</td>
<td>In a list view, shows the entire text value of the multitext value in a list, without truncating it. Without this attribute, the string is truncated based on the UI property Number of characters displayed in list cells which is 40 by default.</td>
</tr>
<tr>
<td>no_update</td>
<td>true/false</td>
<td>table</td>
<td>True for tables in which records are inserted or deleted but not updated. Prevents the system from creating sys_mod_count, sys_updated_by, sys_updated_on fields in the table when created. Does not stop updates of the table. This attribute setting is used to save space on high volume system tables, such as syslog and sys_audit.</td>
</tr>
<tr>
<td>no_view</td>
<td>true/false</td>
<td>any glide_list field</td>
<td>Hides the view-selected item icon.</td>
</tr>
<tr>
<td>Name</td>
<td>Value</td>
<td>Target Element</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------</td>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>onlineAlter</td>
<td>true/false</td>
<td>any table</td>
<td>Tables with the <strong>onlineAlter</strong> attribute perform MySQL database operations using online schema changes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Online schema changes provide a lock-free table upgrade when adding, modifying, or removing columns and when adding or dropping indexes. Without online schema changes, these changes to the database lock write access during execution.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Online schema changes use additional system resources. Oracle databases do not lock tables by default and do not use online schema changes.</td>
</tr>
<tr>
<td>order</td>
<td>numeric value</td>
<td>model variable fields</td>
<td>Used internally only (for model variables).</td>
</tr>
<tr>
<td>pop-up_processor</td>
<td>binary Java class name</td>
<td>any field or table</td>
<td>Specifies a custom pop-up processor for processing the field (or all fields in a table).</td>
</tr>
<tr>
<td>readable</td>
<td>true/false</td>
<td>any conditions field</td>
<td>When true, causes rendering of the conditions field in any list view as a human-readable condition (instead of the encoded query stored in the database).</td>
</tr>
<tr>
<td>ref_ac_columns</td>
<td>list of field names separated by semi-colons</td>
<td>any reference field with an auto completer (see ref_auto_completer)</td>
<td>Specifies the columns whose display values should appear in an auto completion list, in addition to the name. To learn more, see the cmdb_ci field (<em>Configuration Item</em>) on the Incident form for a working example.</td>
</tr>
<tr>
<td>Name</td>
<td>Value</td>
<td>Target Element</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------</td>
<td>---------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ref_ac_columns_search</td>
<td>true/false</td>
<td>any reference field with an auto completer (see ref_auto_completer)</td>
<td>Causes auto-complete to work with all fields specified in the <code>ref_ac_columns</code> attribute. This attribute overrides the default behavior, which searches only the display value column. To learn more, see Configure auto-complete to match text from any reference field.</td>
</tr>
<tr>
<td>ref_ac_display_value</td>
<td>true/false</td>
<td>any reference field with an auto completer (see ref_auto_completer)</td>
<td>Causes the reference field to hide the display value column so that the auto-complete function only matches text from the columns listed in the <code>ref_ac_columns</code> attribute. This feature requires the use of the AJAXTableCompleter class and the <code>ref_ac_columns</code>, <code>ref_ac_columns_search</code>, and <code>ref_ac_display_value</code> attributes. To learn more, see Remove the display value column.</td>
</tr>
<tr>
<td>ref_ac_order_by</td>
<td>field name</td>
<td>any reference field with an auto completer (see ref_auto_completer)</td>
<td>Specifies the column that is used to order the auto completion list.</td>
</tr>
<tr>
<td>Name</td>
<td>Value</td>
<td>Target Element</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------------------------------</td>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ref_auto_completer</td>
<td>JavaScript class name</td>
<td>any reference field</td>
<td>Specifies the name of a JavaScript class (client side) that creates the list auto completion choices. Valid class values include:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• AJAXReferenceCompleter: Matching auto-complete choices appear as a list. Only the display value column of the reference table appears. If there is no other auto-completion class specified, reference fields automatically use this class.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• AJAXTableCompleter: Matching auto-complete choices appear as rows in a table. The display value column of the reference table appears, with any columns listed in the ref_ac_columns attribute.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• AJAXReferenceChoice: Displays matching auto-complete choices as a list. Only the display value column of the reference table, and up to 25 matching choices, appear. If there are more than 25 auto-complete choices, the choices for the AJAXTableCompleter class appear for the reference field instead.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For more information, see Auto-complete for reference fields.</td>
</tr>
<tr>
<td>ref_contributions</td>
<td>UI Macro name list, separated by semicolons (&quot;;&quot;)</td>
<td>any reference field</td>
<td>When the field renders on a form, it invokes the named UI macro.</td>
</tr>
<tr>
<td>ref_decoration_disabled</td>
<td>true/false</td>
<td>any reference field</td>
<td>When set to true, disables the display of the reference icon on a selected field.</td>
</tr>
<tr>
<td>Name</td>
<td>Value</td>
<td>Target Element</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------</td>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ref_list_label</td>
<td>label text</td>
<td>any table</td>
<td>Specifies the title to use in a list banner.</td>
</tr>
<tr>
<td>ref_qual_elements</td>
<td>field name list, separated by semicolons (&quot;;&quot;)</td>
<td>any reference field with a reference_qual field</td>
<td>Specifies a list of fields to send back to the server to get an updated reference.</td>
</tr>
<tr>
<td>ref_sequence</td>
<td>list of fields in referenced table, separated by top hats (^)</td>
<td>any reference field</td>
<td>Specifies the fields in the referenced table used to order the list. This attribute works like an ORDER BY clause in SQL, with each element in ascending order.</td>
</tr>
<tr>
<td>reference_types</td>
<td>list of valid reference types that are clickable separated by semicolons (&quot;;&quot;)</td>
<td>field_name field</td>
<td>Limits the reference fields that appear in the tree to the specified types.</td>
</tr>
<tr>
<td>remoteDependent</td>
<td>name of database and table (like &quot;model.matcher&quot;)</td>
<td>any script field</td>
<td>Defines the remote (such as, in another database) table that the script depends on.</td>
</tr>
<tr>
<td>repeat_type_field</td>
<td>field name</td>
<td>a repeat count field for schedule rotation</td>
<td>Specifies the field that contains the repeat type (daily, weekly, monthly, or yearly).</td>
</tr>
<tr>
<td>ro_collapsible</td>
<td>true/false</td>
<td>any multiline field</td>
<td>If present or true, causes an icon (either a &quot;+&quot; or a &quot;:&quot;) to appear next to the field label, allowing the field itself to be expanded or collapsed.</td>
</tr>
<tr>
<td>Name</td>
<td>Value</td>
<td>Target Element</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------</td>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>scale</td>
<td>integer</td>
<td>decimal field</td>
<td>Sets the number of decimal places to use on a Decimal field type. The default is 2. This attribute is applied to the max length attribute setting for the field. The decimal places for a field are a combination of the max length attribute setting and the scale attribute. For example, if you want four decimal places for the field, you'll need a max length attribute setting of 4, plus the default of 15, or 19. You would set the scale attribute to 4, to indicate the number of decimal places. Six decimal places would require a max length setting of 21, a scale attribute setting of 6, and so on.</td>
</tr>
<tr>
<td>script</td>
<td>a function that returns the contents of the field</td>
<td>any slushbucket field</td>
<td>Enables you to write a script to define what is loaded into the slush bucket field.</td>
</tr>
</tbody>
</table>

**Note:** Increase the max length attribute to a value greater than 15 to increase this attribute.
<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
<th>Target Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>short_label</td>
<td>true/false</td>
<td>any reference field</td>
<td>Long or short labels refer to the label that appears for reference fields on a form. For example, if the reference field contains the caller’s email address, the long label would be Caller Email, while the short label would be Email.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Usually the placement of the reference field on the form makes it clear what the field represents.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• The global property <code>(glide.short.labels)</code> specifies the type of labels that appear for all reference fields on any form.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• You can override the global property for any reference field by setting the <code>short_label=true</code> or <code>long_label=true</code> attribute for the reference field in the dictionary</td>
</tr>
<tr>
<td>show_all_tables</td>
<td>true/false</td>
<td>document ID fields</td>
<td>Enables users to select documents from system tables. For example, <code>sys_script</code> or <code>sys_user</code>. By default, users cannot select records from system tables.</td>
</tr>
<tr>
<td>show_condition_count</td>
<td>true/false</td>
<td>condition fields</td>
<td>Enables or disables the condition count widget to preview how many records are a set of conditions. To learn more, see Add the condition count to a condition field.</td>
</tr>
<tr>
<td>skip_root</td>
<td>true/false</td>
<td>table_name field</td>
<td>If present or true, removes the base table from the list. To learn more, see base_table.</td>
</tr>
<tr>
<td>sla_basis</td>
<td>list of table names separated by semicolons (&quot;;&quot;)</td>
<td>any field of date type (glide_date_time, glide_date, due_date, date, or datetime)</td>
<td>Defines the tables for which this field determines the start (open) time of an SLA.</td>
</tr>
<tr>
<td>Name</td>
<td>Value</td>
<td>Target Element</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>sla_closure</td>
<td>list of table names separated by semicolons (&quot;;&quot;)</td>
<td>any field of date type (glide_date_time, glide_date, due_date, date, or datetime)</td>
<td>Defines the tables for which this field determines the ending (close) time of an SLA.</td>
</tr>
<tr>
<td>slushbucket_ref_no_expand</td>
<td>true/false</td>
<td>any reference field</td>
<td>If present or true, prevents users from expanding the field from a form or list slush bucket.</td>
</tr>
<tr>
<td>smallTable</td>
<td>true/false</td>
<td>any table</td>
<td>If present or true, marks this table as Small (that is, not large) for querying purposes. Without this attribute (or the largeTable attribute), the glide.db.large.threshold property, or a default value of 5,000 determines whether the table is large.</td>
</tr>
<tr>
<td>start_locked</td>
<td>true/false</td>
<td>any glide_list field</td>
<td>Determines whether the field is locked or unlocked by default. Set the value to false to unlock the field by default.</td>
</tr>
<tr>
<td>staticDependent</td>
<td>name of table</td>
<td>any script field</td>
<td>Specifies the table that the script depends on.</td>
</tr>
<tr>
<td>strip_html_in_pdf</td>
<td>true/false</td>
<td>any field</td>
<td>Attempts to remove HTML tags from a field when that field is exported to a PDF. It is most useful on HTML fields.</td>
</tr>
<tr>
<td>synch_attachments</td>
<td>true/false</td>
<td>any table</td>
<td>Similar to update_synch but writes the file attachments of the record to update sets. To learn more, see Index attachments on a table.</td>
</tr>
<tr>
<td>table</td>
<td>name of table</td>
<td>field_name field</td>
<td>Displays the specified table fields.</td>
</tr>
<tr>
<td>tableChoicesScript</td>
<td>name of script include</td>
<td>table_name field</td>
<td>Name of a script include whose process() method returns an array of table names from which to select.</td>
</tr>
<tr>
<td>target_form</td>
<td>name of form</td>
<td>any table</td>
<td>Specifies the alternative form to be used when this table is referenced through a pop-up on a reference field.</td>
</tr>
<tr>
<td>Name</td>
<td>Value</td>
<td>Target Element</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------</td>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>text_index_filter_junk</td>
<td>true/false</td>
<td>any table</td>
<td>Set the value to false to disable the junk filter for the table.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• By default, Zing does not index or search for two-digit numbers and single character words (unless they are Chinese or Japanese characters).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Regenerate the index after disabling the junk filter. This attribute results in a larger table index.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• For optimal performance, do not apply it unless it is required.</td>
</tr>
<tr>
<td>text_search_only</td>
<td>true/false</td>
<td>table_name field</td>
<td>Limits the tables listed to those tables that are searchable by text.</td>
</tr>
<tr>
<td>text_index_translations</td>
<td>true/false</td>
<td>any table</td>
<td>If present or true, forces indexes to be recalculated when translated strings are added. Requires sys-admin role to modify. Automatically set for indexed fields that are translated, and to fields that have a translation and are being indexed. The glide.i18n.force_index system property, which defaults to true, overrides this attribute.</td>
</tr>
<tr>
<td>time_zone_field</td>
<td>name of field containing the time zone</td>
<td>any schedule date/time field</td>
<td>Specifies the field in the parent record that contains the reference time zone for this field.</td>
</tr>
<tr>
<td>timeDimension</td>
<td>true/false</td>
<td>any field of date type (glide_date_time, glide_date, due_date, date, or datetime) in a table subclassed from the task table</td>
<td>If present or true, enables production of time dimension data for use by OLAP (to produce reports based on quarters, weeks, or other time periods).</td>
</tr>
</tbody>
</table>

Note: OLAP functionality has been deprecated.
<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
<th>Target Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tree_picker</td>
<td>true/false</td>
<td>reference field to a hierarchical table</td>
<td>Displays the hierarchy of reference values in a tree display (such as locations).</td>
</tr>
<tr>
<td>ts_weight</td>
<td>integer value</td>
<td>any field</td>
<td>Controls the relative importance of a match in the field for text search. To learn more, see Control Match Relevance By Field.</td>
</tr>
<tr>
<td>types</td>
<td>list of valid element types separated by semicolons (&quot;,&quot;;)</td>
<td>field_name field</td>
<td>Limits the display of fields to the specified types.</td>
</tr>
<tr>
<td>update_synch</td>
<td>true/false</td>
<td>any table</td>
<td>Indicates that changes in the table are tracked in update sets. Administrators cannot modify this attribute. To migrate data, use an instance-to-instance import.</td>
</tr>
<tr>
<td>use_document_viewer</td>
<td>true/false</td>
<td>any table</td>
<td>If present or true, enables users to open supported attachments in a document viewer within the platform, rather than downloading the files directly to their own file system.</td>
</tr>
<tr>
<td>use_workflow</td>
<td>true/false</td>
<td>any table that has delivery plans or uses workflow</td>
<td>If present or true, causes workflow to be used instead of delivery plans.</td>
</tr>
<tr>
<td>user_preference</td>
<td>true/false</td>
<td>any field</td>
<td>If present or true, causes any user preferences to be used instead of the normal default value.</td>
</tr>
</tbody>
</table>

**Modify the Glide durations format**

To convert fields that are displayed in milliseconds (such as 'Resolution Time' on the Incident table) to a duration format (Months/Days/Hours/Seconds), populate the attribute field on the dictionary with: `format=glide_duration`.

Now the value is displayed as a duration in lists and can be utilized in the Configure Calculations functions. This may be useful to illustrate ITIL KPIs such as Mean Time To Repair.

Field Dictionary:
Results in list:
### Schema map for tables

The schema map displays the details of tables and their relationships in a visual manner, allowing administrators to view and easily access different parts of the database schema.

The schema map can also be printed directly from a browser.

Schema relationship types supported, and the colors used for them, are:

<table>
<thead>
<tr>
<th>Relationship type</th>
<th>Color used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Referenced by</td>
<td>Red</td>
</tr>
<tr>
<td>Referencing</td>
<td>Orange</td>
</tr>
<tr>
<td>Extended by</td>
<td>Green</td>
</tr>
<tr>
<td>Extending</td>
<td>Blue</td>
</tr>
</tbody>
</table>

By default, all these types of relationship are displayed, but you can view or hide each type.

### Generate a schema map

Generate a schema map to view and easily access different parts of the database schema.

1. Navigate to **System Definition > Tables & Columns**.
2. In the **Table Names** pane, select a table.
3. Click **Schema map**.

   The schema map for the selected table opens in a separate tab or window.

   If required, you can print this map from the browser.
View the schema map

The schema map shows the selected table in yellow, typically centered, and all tables related to that table, typically shown at the sides.

From this map:

- The check boxes at the top allow you to control which relationships to display. Select or clear a relationship type to display or hide tables with that relationship to the selected table.
- Each related table has a colored bar indicating the relationship to the selected table.
- You can point to the connector lines to display the details of a relationship between the two tables.

**Note:** Since relationships are shown as single lines for simplicity, the diagrams rendered are not entity relationship diagrams.

Using the Table Selector:

To view a schema map as a list, point to the table selector in the right corner:
You can:
- Click a table in the list to scroll the schema map to that table.
- Click the eye icon beside a listed table to hide or show that table in the schema map.
- Click the pin icon in the selector to keep the list open.

Using Related Tables:
Right-click a table node header to display a context menu with these functions:
- **Focus on this table**: Make the selected table the new focus table and redraw the schema map based on the new selection.
  - The new focus table is added as a breadcrumb at the top, allowing you to return to the previous table at any time.
- **Go to list**: Display the list of records for the table.
- **Go to dictionary**: Display the system dictionary, filtered for the selected table.

To hide a related table from view, click the eye icon in the node header (the node can be made visible again with the table selector).

For tables that are part of their own derivation hierarchy, click the expand button (+) in the node header to add their derivation hierarchy to the schema map.

**Viewing More Information**

Click the expand button (+) beside **Columns** to expand the table fields.
The reference fields show a red notation of the table they refer to.

If any tables extend from a table, their columns are displayed in reverse derivation order. For example:

Here, the Server [cmdb_ci_server] table extends from Computer [cmdb_ci_computer], Hardware [cmdb_ci_hardware], and Configuration Item [cmdb_ci], and displays the columns from those tables.

Similarly, the Computer table displays the columns from the Hardware and Configuration Item tables.

**Create a many-to-many relationship**

Many-to-many relationships allow a list to point to a list of entries, rather than to single field.

For example, if a knowledge base article points to a list of related configuration items, it uses a related list. Not all lists can be used as related lists, however. For a list to be related to another list, a many-to-many relationship that refers to both tables must exist.

The Many to Many Definitions [sys_m2m] table allows administrators to create custom many-to-many relationships.

1. In the navigation filter, enter `sys_m2m.list`.
2. Click New.
3. In the **From table** field, specify a parent table.
4. In the **To table** field, specify a child table.
   The Many-to-Many form automatically populates the other fields with suggested values.
5. Optional: Edit other field values, if appropriate. Many-to-Many table names cannot exceed 30 characters.

**Reference default many-to-many relationships**

Some many-to-many relationships are defined by default.

To reference many-to-many relationships that are available in the base system, administrators can enter `sys_collection.list` in the navigation filter.

**Note:** Only use this table to view many-to-many relationships in the base system. To create a new relationship, always use the Many-to-Many Definitions table.

**Database views**

A database view defines table joins for reporting purposes.

For example, a database view can join the Incident table to the Metric Definition and Metric Instance tables. This view can be used to report on incident metrics and may include fields from any of these three tables.

A number of useful database views are installed with the Database View plugin and the Database Views for Service Management plugin. These database views cover most metric reporting needs and greatly reduce the need to define new ones.

**Note:** In general, as the number of tables that are included in the view and the number of records that those tables contain increases, the accumulated impact on performance grows. In addition, to optimize the performance of the database view ensure that the ‘where’ clauses that are defined in the database view are based on indexed fields.

**Limitations**

- Database views cannot be created on tables that participate in table rotation.
- It is not possible to edit data within a database view.
- In a clone request, database view tables cannot be added as a data preserver.

**ACLs and database views**

You do not need to create ACLs on fields in the view. The system honors contextual ACLs (ACLs with a condition or script) that already exist on the underlying table. Non-contextual ACLs (ACLs with only role checks) are still honored just as with previous releases.

To require explicit read ACLs be added to the database views, set the `glide.security.expander.view.legacy` property to `true`. On upgraded instances, add this system property and set it to `true`. See Add a system property.

You can still create additional ACLs on the database views. These ACLs are evaluated last and are always honored.
Database view reserved words

Using the terms may cause unintended or undesirable performance. For more information, see the MySQL reserved words document.

Database view creation

Create a database view to join tables. You can then create a report based on the database view.

Create a database view

Create the database view.
Role required: admin

1. Navigate to System Definition > Database Views.
2. Click New.
   The Database View form appears.
3. Name the view as you would name a new table.
   The application converts capital letters to lower case and spaces to underscores.
4. Provide a label and a plural.
   The Label and Plural fields define how the database view is labeled in lists and forms.

Database view configuration

5. Optional: Provide a description of the database view so that other users know its purpose.
6. Click **Submit**.
   The database view is added to the **Database Views** table.

**Add a table to the database view**

Specify the table to join to the database view.

The **Table** field in the View Table form specifies the table to join to the database view. Assign a **Variable prefix** if you specify a **Where clause** to define the conditions for the join. These conditions can refer to any field, but typically define the join by matching a field in the table to a field in another table that is part of the database view.

When you write the **Where clause**, add the field name to the **Variable prefix** of its table with an underscore. In the **Where clause** pictured below, `mi_id` refers to the **id** field in the Metric Instance [metric_instance] table (mi) and `inc_sys_id` refers to the **sys_id** field in the Incident [incident] table (inc).

**Note:**

- Database views can not be created on tables that participate in table rotation.
- Use only lowercase characters in the **Variable prefix**. Using uppercase characters may prevent you from viewing the database view in a list.

To see an example of using left joins to create a view, see Example left join in creating a database view.
The **Where clause** supports these JavaScript conditional operators:
1. From the Database View form, click **New** on the View Tables related list.
2. Configure the form and add the **Left join** field (a check box) to the form.
3. Click **Save**.
4. Complete the form and select the **Left join** check box.
   - Selecting **Left join** causes the left-hand table in the database view to display all records, even if the join condition does not find a matching record on the right-hand table. Select this check box to view tables that specify a **Where clause**. Selecting **Left join** for view tables without a **Where clause** does not affect the query.
   - Joined tables are ordered left to right from lowest to highest **Order** values. For example of how Order relates to joined tables, see the View Tables image in **Test the database view**.
5. Click **Submit**.
6. Personalize the **View Tables** related list to show the **Left join** column.
   - The **Left join** field is **true**.
7. Click a record to view a table.
   - The View Table form appears.
8. To add an OR to your Where clause, use ||.

For example, to query all incidents related to RFCs OR all incidents that are the parent of a change request, use the following syntax:

```
inc_rfc = chg_sys_id || chg_parent = inc_sys_id
```

### Database view where clause

<table>
<thead>
<tr>
<th>Table</th>
<th>Incident [incident]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order</td>
<td>100</td>
</tr>
</tbody>
</table>

| Where clause | inc_rfc = chg_sys_id || chg_parent = inc_sys_id |

**Example left join in creating a database view**

This example shows the proper settings when using left-joins to add tables to a database view.

Role required: admin

The following procedure shows how to create a database view that includes a list of Catalog Tasks and their parents. Most of the steps take place on the following page.
1. Create a database view.
2. On the Database Views page, click the view you created. The Database View page appears. In the View Tables table, you specify the tables you want in the database view.

3. In the **View Tables** table, click **New**. The View Table form appears.

4. Add a **Left join** check box to the form by configuring it.

5. Add the Catalog Task [sc_task] table to the database view by filling in the form with the following data and then clicking **Submit**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>Catalog Task [sc_task]</td>
</tr>
<tr>
<td>Variable prefix</td>
<td>cat</td>
</tr>
<tr>
<td>Order</td>
<td>100</td>
</tr>
<tr>
<td>Where clause</td>
<td>Leave blank</td>
</tr>
</tbody>
</table>

   The Database View page appears with the Catalog Task table in the View Tables table.

6. In the **View Tables** table, click **New** and add the Requested Item [sc_req_item] table to the database view by filling in the form with the following data and then clicking **Submit**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>Requested Item [sc_req_item]</td>
</tr>
<tr>
<td>Variable prefix</td>
<td>item</td>
</tr>
<tr>
<td>Order</td>
<td>200</td>
</tr>
<tr>
<td>Where clause</td>
<td>cat_parent=item_sys_id</td>
</tr>
<tr>
<td>Left join check box</td>
<td>True</td>
</tr>
</tbody>
</table>

   The Database View page appears with the Requested Item table in the View Tables table.

7. In the **View Tables** table, click **New** and add the Request [sc_request] table to the database view by filling in the form with the following data and then clicking **Submit**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>Request [sc_request]</td>
</tr>
<tr>
<td>Variable prefix</td>
<td>req</td>
</tr>
<tr>
<td>Order</td>
<td>300</td>
</tr>
<tr>
<td>Where clause</td>
<td>cat_parent=req_sys_id</td>
</tr>
<tr>
<td>Left join check box</td>
<td>True</td>
</tr>
</tbody>
</table>

   The Database View page appears with the Request table in the View Tables table.

8. In the **View Tables** table, click **New** and add the User [sys_user] table to the database view by filling in the form with the following data and then clicking **Submit**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>User [sys_user]</td>
</tr>
<tr>
<td>Variable prefix</td>
<td>user</td>
</tr>
<tr>
<td>Order</td>
<td>400</td>
</tr>
<tr>
<td>Field</td>
<td>Value</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Where clause</td>
<td>cat_opened_by=user_sys_id</td>
</tr>
<tr>
<td>Left join check box</td>
<td>False</td>
</tr>
</tbody>
</table>

- The Database View page appears with the User table in the View Tables table.
- If the parent record of Catalog Task is a Requested Item, all the fields in the Request table will be blank.
- If the parent record is a Request, all the fields in Requested Item will be blank.
- Because of the two left joins, the Catalog Task record returns even if the parent is empty or is not a Requested Item or Request.
- Because User is not a left join, there must be a matching user in sys_user for the row’s Opened By field for the Catalog Task row to return.

9. Optionally, perform the following steps to experiment and learn more about how left joins impact database views. If you make the left join in:

- User true, rows that have an empty **Created By** return.
- Requested Item false, only Catalog Tasks that have a Requested Item as a parent return.
- Request false, only Catalog Tasks that have a Request as a parent return.
- Requested Item and Request false, no rows return because nothing can have a Requested Item and a Request as parents.

### Specify a field to return

Use the View Field form to restrict or specify a field that you want returned by the joined table.

If no fields are defined in the View Fields list, all fields are returned. If any fields are defined, then only those fields are returned.

![View Field Form](image)

**View Fields list**

When you restrict the fields returned by creating View Field records, you must create a record for the join field from the **Where clause** in the parent record. If you omit a record for this field, it cannot be returned, and the join fails. In the previous example, the **Where clause** uses the **sys_id** field from the Incident table to establish the join. For the join to succeed with a restricted field list, you must include a record for the **sys_id** field.
Relabel a column

In some cases, two different tables may have fields of the same name that are both important (such as two tables with a sys_updated_on field). You must rename one of these fields.

To create clear reports, relabel the fields on the Database View [sys_db_view] table without changing the names of the fields.

1. Navigate to System Definition > Language File.
2. Click New.
3. Fill in the form as follows:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>Name of the database view</td>
</tr>
<tr>
<td>Label</td>
<td>Display label</td>
</tr>
<tr>
<td>Plural</td>
<td>Plural form of the display label</td>
</tr>
<tr>
<td>Element</td>
<td>Name of the field on the database view</td>
</tr>
</tbody>
</table>

Specify the number of records to return

Specify the number of records to return for a database view.

A property called glide.db.max_view_records controls the maximum number of rows returned when running a GlideRecord query in a script. The default value for this property is 10000. To change this value, add the property to the System Property [sys_properties] table and edit the number of rows to return.

This property only applies when querying a database view table in a script. When displaying the database view table in a list or report, this property does not apply.
Test the database view

Verify that the database view works correctly.

After the new view is defined, test it by clicking Try It under Related Links on the Database View form.

If you do not see the Try It link, the tables necessary for the view do not exist. If this occurs, it is possible that you did not activate the necessary plugins to create the supporting tables. When tables are present to support the view, the form looks like this:
**Database View**

**pm_project_sla**

<table>
<thead>
<tr>
<th>Name</th>
<th>pm_project_sla</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Join pm_project to sla(task_sla) to report on things like project names by sla.</td>
</tr>
</tbody>
</table>

**Related Links**

**Try It**

**View Tables**

<table>
<thead>
<tr>
<th>View = pm_project_sla</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table: task_sla</td>
</tr>
<tr>
<td>Table: pm_project</td>
</tr>
<tr>
<td>Order: taskslatable</td>
</tr>
<tr>
<td>Order: pmp</td>
</tr>
</tbody>
</table>

**Note:** Database views tables are not included in FTP exports.
Use disjunctions in complex queries

ServiceNow performs conjunction statements before disjunction statements in a query.

When you create a complex query, you must use parenthesis around disjunctions where appropriate to ensure proper grouping of query elements. For example, you must use parenthesis in the query `(md_table = 'incident' || md_table = 'task') && mi_definition = md_sys_id && mi_id = inc_sys_id`. Removing the parenthesis from this query returns all records where the md_table value is incident.

Database views in the base system

Certain views are included in the base system with the Database Views and Database Views for Service Management plugins.

### Database views

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>change_request_metric</td>
<td>Join change to metric definition to metric instance, creating a view that can be reported on for things like: Changes that were closed by category.</td>
<td>Change Metric</td>
</tr>
<tr>
<td>change_request_sla</td>
<td>Join change_request to sla(task_sla), creating a view that can be reported on for things things like change request resolved by sla per change category.</td>
<td>Change Request SLA</td>
</tr>
<tr>
<td>change_task_metric</td>
<td>Join change task to metric definition to metric instance, creating a view that can be reported on for things like: Change tasks that were closed by change state</td>
<td>Change Task Metric</td>
</tr>
<tr>
<td>change_task_sla</td>
<td>Join change_task to sla(task_sla), creating a view that can be reported on for things things like change tasks resolved by sla.</td>
<td>Change Task SLA</td>
</tr>
<tr>
<td>change_task_time_worked</td>
<td>Join change task to task time worked to pull time worked entries associated with incidents.</td>
<td>Change Task Time Worked</td>
</tr>
<tr>
<td>incident_metric</td>
<td>Join incident to metric definition to metric instance creating a view that can be reported on for things like: Incidents that were resolved on the first call by category</td>
<td>Incident Metric</td>
</tr>
<tr>
<td>incident_sla</td>
<td>Join incident to sla(task_sla) to report on things like incidents resolved by sla per incident category.</td>
<td>Incident SLA</td>
</tr>
<tr>
<td>incident_time_worked</td>
<td>Join incident to task time worked to pull time worked entries associated with incidents.</td>
<td>Incident Time Worked</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Label</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>pm_project_metric</td>
<td>Join pm_project to metric definition to metric instance creating a view that can be reported on for things like: Projects that were closed by name or date.</td>
<td>Project Metric</td>
</tr>
<tr>
<td>pm_project_sla</td>
<td>Join pm_project to sla(task_sla) to report on things like project names by sla.</td>
<td>Project SLA</td>
</tr>
<tr>
<td>pm_project_task_metric</td>
<td>Join pm_project_task to metric definition to metric instance creating a view that can be reported on for things like: Project tasks that were closed by name or date.</td>
<td>Project Task Metric</td>
</tr>
<tr>
<td>pm_project_task_sla</td>
<td>Join pm_project to sla(task_sla) to report on things like release tasks by sla.</td>
<td>Project Task SLA</td>
</tr>
<tr>
<td>pm_project_task_time_worked</td>
<td>Join pm_project_task to task time worked to pull time worked entries associated with project tasks.</td>
<td>Project Task Time Worked</td>
</tr>
<tr>
<td>problem_metric</td>
<td>Join problem to metric definition to metric instance creating a view that can be reported on for things like: Problems that were resolved on the first call by category.</td>
<td>Problem Metric</td>
</tr>
<tr>
<td>problem_sla</td>
<td>Join problem to sla(task_sla) to report on things like problems resolved by sla per problem state.</td>
<td>Problem SLA</td>
</tr>
<tr>
<td>release_feature_metric</td>
<td>Join release_feature to metric definition to metric instance creating a view that can be reported on for things like: Release Features that were closed by product.</td>
<td>Release Feature Metric</td>
</tr>
<tr>
<td>release_project_metric</td>
<td>Join release_project to metric definition to metric instance creating a view that can be reported on for things like: Releases that were closed by category.</td>
<td>Release Metric</td>
</tr>
<tr>
<td>release_task_metric</td>
<td>Join release_task to metric definition to metric instance creating a view that can be reported on for things like: Release Features that were closed by feature.</td>
<td>Release Task Metric</td>
</tr>
<tr>
<td>release_task_sla</td>
<td>Join release_task to sla(task_sla) to report on things like release tasks by sla.</td>
<td>Release Task SLA</td>
</tr>
<tr>
<td>sc_request_metric</td>
<td>Join sc_request to metric definition to metric instance creating a view that can be reported on for things like: Requests that were closed by category.</td>
<td>Catalog Request Metric</td>
</tr>
</tbody>
</table>
List administration

Administrators control the data presented to end users in a list, the controls that appear, and the behavior of the controls.

Note: For information about using lists, see Lists.

List configuration

Users with the appropriate roles can configure various aspects of lists. Configuration changes apply to all users.

With list configuration, you can add, remove, and reorder list columns. You can configure calculations to appear under columns. You can also hide controls and define access conditions by role for existing list controls. Configuring lists is called personalizing lists in versions prior to the Fuji release.

Note: Configuring a list in this way modifies the list for all users. To make changes to a list that are visible to you only, see Personal lists.

Configure the list layout

You can configure a list to choose which columns appear in a list, create list views, and create fields on the table.

Role required: personalize_list

1. Navigate to the list you want to configure.
2. Select the view to configure by performing the appropriate action for the list version.

<table>
<thead>
<tr>
<th>Version</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>List v2</td>
<td>Open the list title menu and select View &gt; (view name).</td>
</tr>
<tr>
<td>List v3</td>
<td>Open the list title menu and select Change View, and then click the name of the view.</td>
</tr>
</tbody>
</table>
3. Open the list configuration page by performing the appropriate action for the list version.

<table>
<thead>
<tr>
<th>Version</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>List v2</td>
<td>Right-click any column heading and select <strong>Configure &gt; List Layout</strong>.</td>
</tr>
<tr>
<td>List v3</td>
<td>Open the list title menu and select <strong>List Layout</strong>.</td>
</tr>
</tbody>
</table>

4. Use the slushbucket to select the columns and the order of appearance.

   In lists using List v2, the first non-reference field automatically links to the form view of the record. For this reason, consider using the record number as the first column in the list layout.

   In lists using List v3, the first field automatically links to the form view of the record regardless of whether or not it is a reference field. In this cases, an icon appears to the right of the text. This icon links to the referenced record rather than the record displayed on the current list view.

5. Click **Save**.

   **Note:** If you create a personal list and then configure the list view differently, the changes do not appear until you reset your personal list to column defaults.

---

**Add an extended field to a base table list**

Administrators can configure a property that determines whether fields on extended tables can be added to a parent table list. For example, when this feature is enabled, you can view and filter on the **Caller** field, from the Incident table, on a Task table list.

Role required: admin

   **Note:** Enabling this property does not show the extended table fields in the personalize list.

1. Navigate to **System Properties > UI Properties**.
2. Locate the property **Allow base table lists (task, cmdb_ci, etc.) to include extended table fields (incident_state, os_version, etc.), and allow filtering on extended table fields (glide.ui.list.allow_extended_fields)**.
3. Select the check box to enable extended fields on parent table lists. Clear the check box to disable the feature.
4. Click **Save**.

---

**Configure list calculations in List v2**

In List v2, you can configure list calculations for columns, which calculate column totals, minimums, maximums, and averages.

Role required: personalize_list

You can configure list calculations for multiple columns in the same list. List calculations apply only to the view of the list in which they are configured. All users can see configured list calculations.
Note: List calculations are available in list reports.

1. In a list of records, right-click the header of a numeric column you want to evaluate with list calculations.
2. Select Configure > List Calculations.
   The list calculation window appears.

3. Select one or more of the following list calculation options:
   - Total value (not available for string, date, or date/time fields)
   - Minimum value
   - Maximum value
   - Average value (not available for string, date, or date/time fields)

4. Click OK.
   The calculations appear below the last record in the column. If the list is grouped, in addition to the overall calculations at the bottom of the list, group calculations appear below the last record in each group.

Omit record count in a list

Speed up how fast lists load by removing the calculation of the total number of records in a list.

Role required: workspace_admin

Calculating the total number of records included in a list that's filtered from large tables can take a long time. Platform displays the total number of records in the list.

To load lists faster, you can remove the page calculation for all or only specified filtered lists. When you remove the calculation, the total record count is not displayed and the double arrow icon is grayed out.
1. Open a list, for example navigate to Incident > All.
2. Right-click a header in the list and navigate to Configure > List Control.
3. Select Remove pagination count.
4. Optional: To omit the record count only in specific view:
   a) Select Remove pagination count for specific views.
   b) Beside Specific list of views prevented from getting full record count, click the lock icon.
   c) Click the search icon and select the view where platform omits the page count.
   d) Repeat the previous step for as many views as necessary.
5. Click Update.

Configure list controls
You can configure list controls, such as buttons and filters.
Role required: personalize_control
1. Open a list.
2. Open the list configuration page by performing the appropriate action for the list version.

<table>
<thead>
<tr>
<th>Version</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>List v2</td>
<td>Right-click any column heading and select Configure &gt; List Control.</td>
</tr>
<tr>
<td>List v3</td>
<td>Open the list title menu and select List Control.</td>
</tr>
</tbody>
</table>

The List Control form appears.
3. Complete the form.

Note: The list control fields that are available for embedded lists are more limited. Unless otherwise noted, the list control fields in the following table are available for both standard and embedded lists.

List Control form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>Name of the table for the list or related list. For example, Change Request [change_request]. The system automatically sets this value.</td>
</tr>
<tr>
<td>Related list</td>
<td>Name of the table and field that define the related list. For example, sysapproval_approver.sysapproval. The system automatically sets this value.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Label</td>
<td>Label to display for this list. Allows an admin to customize the label for a related list or list. If not supplied, the default plural label for the file is used. For example, the label for the Incident table would be <em>Incidents</em>.</td>
</tr>
<tr>
<td>Omit new button</td>
<td>Option to prevent the <strong>New</strong> button from displaying on this list. Clear the check box to display the <strong>New</strong> button or to control the <strong>New</strong> button with roles (<strong>New roles</strong> field). This field is available for standard lists only.</td>
</tr>
<tr>
<td>Omit edit button</td>
<td>Option to prevent the <strong>Edit</strong> button from displaying on this list. Clear this check box to display the <strong>Edit</strong> button or to control the <strong>Edit</strong> button with roles (<strong>New roles</strong> field). The <strong>Edit</strong> button does not apply to all lists. This field is available for standard lists only.</td>
</tr>
<tr>
<td>Omit if empty</td>
<td>Option to omit the Related List from the form entirely (no header) if there are no entries for the Related List.</td>
</tr>
<tr>
<td>Omit columns if empty</td>
<td>Option for a top-level list to omit the column headers AND filters/breadcrumbs for an empty column.</td>
</tr>
<tr>
<td>Omit filters</td>
<td>Option to hide filters or breadcrumbs for this list. Clear this check box if you always want filters or breadcrumbs or to control filters/breadcrumbs with roles (<strong>Filter roles</strong> field). This field is available for standard lists only.</td>
</tr>
<tr>
<td>Omit links</td>
<td>Option to hide links for fields that reference other files in this list. Leave this button unchecked to generate links or to control the use of links with roles (<strong>Link roles</strong> field).</td>
</tr>
<tr>
<td>Omit drill-down link</td>
<td>Option to disable the link to the record from the first column in list view. Users can still select the reference icon to access the record. This field is available for standard lists only.</td>
</tr>
<tr>
<td>Hierarchical lists</td>
<td><strong>Hierarchical list</strong> inserted into a record list. Hierarchical lists enable a user to view the contents of a record's related lists without leaving the record list form. This field is available for standard lists only.</td>
</tr>
</tbody>
</table>

**Note:** Enabling this setting renders the list incompatible with List v3. The list always renders in List v2, even if List v3 is enabled.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>List edit type</td>
<td>Ability for the user to edit values directly in individual cells in a list. The options are:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Save immediately (cell edit mode):</strong> enables cell editing. The entire row is saved when the user enters a new value.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Save data by rows:</strong> enables cell editing. The row is saved only when the user navigates away from the row or selects the <strong>Save</strong> icon (✓).</td>
</tr>
<tr>
<td></td>
<td>- <strong>Disable list editing:</strong> prevents users from editing cells in the list.</td>
</tr>
<tr>
<td></td>
<td>This field is available for standard lists only.</td>
</tr>
<tr>
<td>List edit tag</td>
<td>Unique tag that is sent to a reference qualifier as the script variable <code>listEditRefQualTag</code>. Enter an arbitrary string of letters or numbers.</td>
</tr>
<tr>
<td>List edit insert row</td>
<td>Ability for a user to create records in list view. When it is enabled, an empty row appears at the bottom of the list.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Enabling this setting renders the list incompatible with List v3. The list always renders in List v2, even if List v3 is enabled.</td>
</tr>
<tr>
<td>Remove pagination count</td>
<td>Option to remove pagination count from the list.</td>
</tr>
<tr>
<td>Disable Natural Language Query (NLQ)</td>
<td>Option to disable the NLQ filter in specific lists when NLQ on lists is enabled in the instance. The NLQ filter enables you to use natural language to filter lists instead of using the condition builder. For more information on NLQ filters, see Natural Language Query.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> When the system property <code>(com.snc.listv2.nlq.lists.enabled)</code> is set to <code>false</code>, the query destructs. Text entered in the search replaces existing conditions.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Application</td>
<td>Scope of this setting's applicability. Global means that all workspaces can use this setting.</td>
</tr>
<tr>
<td>New roles</td>
<td>User roles that can access the <strong>New</strong> button on this list. Leave the field blank to enable all users to access the <strong>New</strong> button. This option does not apply to embedded lists, which do not contain <strong>New</strong> buttons.</td>
</tr>
<tr>
<td>Filter roles</td>
<td>User roles required to have the filter appear in the list. This field is available for standard lists only.</td>
</tr>
<tr>
<td>Link roles</td>
<td>User roles required to have links generated for fields that reference other files.</td>
</tr>
</tbody>
</table>

**Example of configuring list controls**

The following example shows how to configure a list of related incidents in a problem record to suit specific business needs.

Role required: personalize_control

In this example, a related list label is configured to say Child Incidents, not just Incidents. The related list is also configured to remove the **New** button to prevent users from creating incidents from the Problem form.

1. Navigate to a problem record.
2. Open the list context menu in the **Incidents** related list and select **Configure > List Control**.
3. On the List Control form, change the **Label** field to Child Incidents.
4. Select the **Omit new button** check box.
5. Select Submit to save your changes and return to the previous record, in this case, the problem record.

In the problem record, the label for the embedded incident list has changed and the **New** button is no longer available.

**Advanced list control with scripts**

You can write scripts to specify which list elements, such as links, filters, and buttons, are present.

These scripts can react to the record that is being displayed. For related list controls, the global variable `parent` identifies the parent record. For primary lists, there is no parent record.

Configure the List Control form and add the script field that you need:

- **Omit Columns Condition**: If there are no conditions, omit column headings.
- **Omit Edit Condition**: Omit the **Edit** button.
- **Omit Empty Condition**: If there are no conditions, omit the list header.
- **Omit Filter Condition**: Omit the list filter.
- **Omit Links Condition**: Omit related links.
- **Omit New Condition**: Omit the **New** button.

In these script fields, if the script evaluates to `true`, the item is omitted. The following script is an example that you can use on the **Affected CIs** related list to show only the **Edit** button if the parent task is active. This script is placed in the **Omit Edit Condition** script field.

```javascript
var answer;
if (parent.active == true) {
  // Add code here to set 'answer' to true or false
}
```
Configure a list UI action

You can create a UI action that opens the slushbucket interface to customize lists in the list view.

Role required: ui_action_admin

1. Navigate to System Definition > UI Actions.
2. Click New.
3. In the Table field, select the List [sys_ui_list] table.
4. Select the List context menu check box.
5. Ensure the Active check box is selected.
6. Paste the following script in the Script field:

   ```javascript
   var url = "slushbucket.do?sysparm_form=list&sysparm_list=" + current.
   name + "&sysparm_view=" + current. view. name;
   url += "&sysparm_collection=" + current. parent +
   "&sysparm_collection_relationship=" + current. relationship;
   url += "&sysparm_referring_url=sys_ui_view.do?sys_id=" + current. view.
   toString () ;
   action. setRedirectURL (url ) ;
   ```
7. Click Submit.

Controlling the sort sequence used to display lists

All lists have a default sort sequence based on the type of fields present in the list.

When a user displays a list for the first time, it is sorted by one of the following items.

- The ORDERBY arguments found the URL. (See the following section on source order control.)
- The <table>.db.order and <table>.db.order.direction user preferences.
- The isOrder dictionary attribute.
- The Order field if one is present in the table.
- The Number field if one is present in the table.
- The Name field if one is present in the table.
- The field specified as the display field for the table.

Note: The task table is an exception to the preceding sequence. Task and tables extended from task use the Number field when no URL arguments or user preferences are found.

Setting default order with user preferences

The <table>.db.order and <table>.db.order.direction user preferences determine the field and sort direction seen by the user. A default sort can be created by creating user preference records with no value in the User field and checking the System check box. This preference is applied to any users who do not have their own preference.
Setting the default sort order in the system dictionary

An administrator can set the sort order of records displayed for a table in the system dictionary when there is no other sort specified. This is done by adding an attribute called `isOrder` with a value of `true` to the dictionary entry of the desired field. This sort is the sort order presented to all users initially. Once a user sorts a list, that user preference is saved, and the list is always sorted for that user based on the previous sorting preference.

**Note:** `isOrder` can define which field is used for list sorting, but cannot control the sort direction.

Sort order control

For any list, if the user has clicked a column header to sort by that column, then that action is remembered. The next time that list is displayed, the same field is used to order the list.

This remembered sort field can be overridden by adding a `sysparm_order` specification to the definition of the module. For example, if each time News is displayed, you want the new items listed in order of importance, then the News module can be updated accordingly.

```
&sysparm_order=importance
```

Set module sort order to the Importance field value

The actual order (ascending or descending) can be specified by adding a `sysparm_order_direction` specification. Here are two examples of sorting a list by the `sys_created_on` field, one ascending and one descending:

```
&sysparm_order=sys_created_on &sysparm_order_direction=desc
&sysparm_order=sys_created_on &sysparm_order_direction=asc
```

Sort by multiple fields

To sort a list by multiple fields, remove everything from the filter field and place it in the arguments field. For example, if the filter specifies `[Active] [is] [true]` and you want to sort by category and subcategory, remove the condition and put the following in the module arguments:

```
active=true^ORDERBYcategory^ORDERBYsubcategory
```

This argument first orders by the category and then orders by the subcategory. If you want any field to be a descending sort, then change `ORDERBY` to be `ORDERBYDESC`.

List editor administration

The list editor allows users to edit field values directly from a list without navigating to a form.

Administrators can manage this feature by using the following options. Some of the options are not supported in List v3.

- Configure global properties
- Configure list control settings for a table
- Configure contextual security rules
- Manage user preferences (List v2 only)

**Warning:** In List v2, the list editor does not enforce client scripts or UI policies. In List v3, the list editor enforces UI policies and mandatory dictionary attributes, but not client scripts. Allowing list editing with client scripts running on fields in a form can result in incorrect data being saved to the record. For systems in which client scripts or UI policies apply to forms, consider disabling list editing or creating appropriate business rules or access control to control the setting of values in the list editor. See Use business rules and client scripts to control field values for information on managing form and list editing.

**Configure list editor properties**

You can configure list editor properties that control whether lists can be edited, and, for List v2, which field types cannot be edited.

Role required: admin

1. Navigate to System Properties > UI Properties.
2. To disable list editing, set the Enable list editing (glide.ui.list_edit) property to No by clearing the check box.
   - This property is enabled by default, and it globally enables list editing. When you disable it, the list editor is disabled globally.
3. To configure the field types that cannot be edited for v2 lists, complete the following steps.
   a) Locate the List of element types (comma-separated) that cannot be edited in the list editor (glide.ui.list_edit_ignore_types) property. It contains several element types that cannot be edited by default.
   
   **Note:** This property does not impact v3 lists. There is no equivalent property for List v3.

   The following field types are not editable from the list editor by default.
   - Conditions [conditions]
   - Currency [currency]
   - Document ID [document_id]
   - Field List [field_list]
   - HTML [html]
   - Image [user_image]
   - List [glide_list]
   - Price [price]
   - Template Value [template_value]
   - Time [glide_time]
   - User Roles [user_roles]
   - Video [video]
   
   b) Add any other field types you want to disable to the end of the list, separated by a comma.

4. Click Save.

**Configure list control settings for the list editor**

You can configure the list control settings that affect the list editor.

Role required: personalize_control
**List control settings** customize the behavior of list functions for a table.

1. Navigate to a list view for the desired table.
2. Open the list configuration page by performing the appropriate action for the list version.

<table>
<thead>
<tr>
<th>Version</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>List v2</td>
<td>Right-click any column heading and select <strong>Configure &gt; List Control</strong>.</td>
</tr>
<tr>
<td>List v3</td>
<td>Open the list title menu and select <strong>List Control</strong>.</td>
</tr>
</tbody>
</table>

3. On the List Control form, select the desired settings.

**List control settings for the list editor**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>List edit type</td>
<td>Ability for the user to edit values directly in individual cells in a list. The options are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Save immediately (cell edit mode)</strong>: enables cell editing. The entire row is saved when the user enters a new value.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Save data by rows</strong>: enables cell editing. The row is saved only when the user navigates away from the row or selects the <strong>Save</strong> icon (✔). This mode allows the user to modify multiple values before saving a record.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disable list editing</strong>: prevents users from editing cells in the list.</td>
</tr>
<tr>
<td>List edit insert row</td>
<td>Ability for a user to create records in list view. When it is enabled, an empty row appears at the bottom of the list.</td>
</tr>
</tbody>
</table>

Note: Enabling this setting renders the list incompatible with List v3. The list always renders in List v2, even if List v3 is enabled.

4. Click **Update**.
Configuring contextual security for the list editor

The list editor enforces existing access control rules (ACLs) and additional security controls to restrict editing from a list.

The list_edit security operation specifically controls the ability to edit information in a list. Apply this operation in the same manner as the write operation to limit list editing for fields that require the user to navigate to the form. Reasons you may require a user to edit a field in a form include complex UI policy constraints or other policies you have in place.

The list_edit security operation specifically controls the ability to edit information in a list. Apply this operation in the same manner as the write operation to limit list editing for fields that require the user to navigate to the form. Reasons you may require a user to edit a field in a form include complex UI policy constraints or other policies you have in place.

• write and list_edit access to the field
• write and list_edit access to any dependent fields of the field
• write and list_edit access to any fields that depend on the field being edited

To configure access controls, navigate to System Security > Access Controls. The following examples use the list_edit security operation to restrict list editing in certain contexts.
Example - Restrict a table

This access control prevents everyone from editing all fields in the Incident table in a list.

Restrict the Incident Table

- **Type**: record
- **Operation**: list_edit
- **Name Incident**: [incident]
- **Admin overrides**: Clear the check box.
- **Script**: `answer = false;`
**Example - Restrict a field**

This access control prevents everyone except an administrator from editing the Short Description field of an incident record in a list.

**Restrict the Incident Short Description**

- **Type:** record
- **Operation:** list_edit
- **Name:** Incident [incident], Short Description
- **Admin overrides:** Select the check box.
- **Script:**

  ```javascript
  answer = false;
  ```
Example - Restrict a field with a script

This access control prevents everyone from editing an incident with a category of Software in a list. It is defined by a script.

Restrict Software Incidents

- **Type**: record
- **Operation**: list_edit
- **Name Incident**: [incident]
- **Admin overrides**: Clear the check box.
- **Script**:

```java
if (current.category == 'software')
    answer = false;
else
    answer = true;
```
Example - Restrict a field with a condition

This access control prevents everyone from editing a Critical Incident in a list. It is defined by a condition.

Restrict Critical Incidents

- **Type:** record
- **Operation:** list_edit
- **Name Incident:** [incident]
- **Admin overrides:** Clear the check box.
- **Condition:** Priority is not 1 - Critical

User preferences for v2 list editing

Users can set user preferences for v2 list editing by personalizing a list (available when the list mechanic is activated). To view and manage list editor user preferences, navigate to **User Administration > User Preferences.**

**Note:** These user preferences do not apply to v3 lists. There are no equivalent user preferences for List v3.
User preferences for v2 list editing

<table>
<thead>
<tr>
<th>User preference name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>list_edit_enable</td>
<td>Set the value to <strong>true</strong> to enable or <strong>false</strong> to disable list editing. Default value is <strong>true</strong>.</td>
</tr>
<tr>
<td>list_edit_double</td>
<td>Set the value to <strong>true</strong> for double-click or <strong>false</strong> for single-click. Default value is <strong>true</strong>.</td>
</tr>
</tbody>
</table>

**Personal list administration**

Users can customize the layout for any list view by personalizing a list. Administrators can configure options related to list personalization.

In List v2, administrators can also disable or restrict access to list personalization. This functionality is not supported in List v3.

**Enable or disable personal lists in List v2**

You can enable or disable List v2 personal lists through the UI Macros module.

Role required: ui_macro_admin

**Note:** This functionality does not apply to List v3. Personal lists are not controlled by the list mechanic in List v3 and are always enabled.

1. Navigate to System UI > UI Macros.
2. Activate (or deactivate) the list_mechanic2 UI macro.

**Control which roles can personalize lists in List v2**

You can control who can create personal lists in List v2.

Role required: admin

**Note:** This functionality does not apply to List v3. All users can personalize v3 lists.

1. Navigate to System Properties > UI Properties.
2. Locate the property labeled List of roles (comma-separated) that can use Personal Lists. If blank, all can use (glide.ui.list_mechanic.roles).
3. Enter the roles for which personal lists are available, separated by commas, or leave the field blank to allow access for all users (default).

**Manage personal lists**

Administrators can manage personal lists.

Role required: admin

1. Navigate to System UI > Lists.
2. Personal lists have a user value in the **User** field.
Administer detail rows

Detail rows provide additional information about records in a list.

Role required: admin

To display detail rows, an administrator must enable them globally and add them to lists.

**Note:** Detail rows are supported in UI15 and up. Detail rows are not supported in List v3.

1. **To enable detail rows,** add a new system property with the following field values.

<table>
<thead>
<tr>
<th>Name</th>
<th>glide.ui.list.detail_row</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>true</td>
</tr>
<tr>
<td>Value</td>
<td>true</td>
</tr>
</tbody>
</table>

2. **To add detail rows to a list,** complete the following steps.

   a) **Add the `detail_row` dictionary attribute** to the table.

      Specify the name of the field to display in the following format:** detail_row=short_description **

   b) **Use the `all_tables` element descriptor with the `detail_row` attribute** to display detail rows for all child tables that contain the designated field.

      For example, `all_tables.detail_row=short_description` is on the Task [task] table by default, so the short description detail row appears in lists for Incident [incident], Problem [problem], and other child tables unless you set `detail_row` to a different field for each one.

Restrict filters and breadcrumbs with fixed queries

The record list view allows users to navigate to different subsets of a table using breadcrumbs and filters. You can limit access to parts of the table by restricting active links in breadcrumbs or by suppressing breadcrumbs and filters for specific roles.

Role required: admin

A breadcrumb option enables an administrator to control the base view of a record list presented to users. By adding a fixed query to the argument for a module, an administrator can prevent users from expanding their view past a specified starting point. The argument for this fixed query is written as `&sysparm_fixed_query=active=true`. A use case for this query is to prevent users from using the breadcrumbs to switch a list of open incidents to a list of all incidents. When users select **Incident > Open**, they are limited to viewing and filtering a list of open (active=true) incidents.

**Note:** A new Create ACL allows all users to save filters by default. This overrides any custom ACLs in place if administrators are restricting filter access. The new ACL gives all users access to the User field by default, and access to the Group field only if users have the filter_group role and are in the currently selected group.

1. **Perform the appropriate action** for your version of the UI:

<table>
<thead>
<tr>
<th>UI16</th>
<th>Point to the application menu that contains the module to edit and click the edit application (pencil) icon.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To open the module directly, point to the module and click the edit module (pencil) icon.</td>
</tr>
</tbody>
</table>
2. Select the module to edit.
   For example, select **Open**.

3. In the **Link Type** section of the Module form, select **List of Records** for the **Link type**.

4. Delete the **Active is true** filter, if present.
5. Add `&sysparm_fixed_query=active=true` to the **Arguments** field and update the record.
6. Navigate to **Incidents > Open** and examine the breadcrumbs.

The **Active=true** link is the widest view permitted in the list of Open incidents shown. The breadcrumb for **All** is not a link because of the fixed query.

---

**Suppress filters and breadcrumbs with list controls**

Use list controls to suppress filters and breadcrumbs on defined tables for users with specific roles.

Role required: personalize_control

1. Navigate to the list view of the table to restrict breadcrumbs.

2. Open list control by performing the appropriate action for the list version.

<table>
<thead>
<tr>
<th>Version</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>List v2</td>
<td>Right-click any column header and select <strong>Configure &gt; List Control</strong>.</td>
</tr>
<tr>
<td>List v3</td>
<td>Open the list title menu and select <strong>List Control</strong>.</td>
</tr>
</tbody>
</table>

You can also navigate to **System UI > List Control**.

3. On the List Control form, select the **Omit Filters** check box. Clear the check box to include filters.

The **Filter Roles** field allows an administrator to specify certain roles that can see the filters.

---

**Use script includes to suppress filters and breadcrumbs**

You can use a script to restrict filters and breadcrumbs to specific roles, either on a per-table or global basis. Using a script is an advanced option that offers additional flexibility compared to using list control.

Using a script include requires knowledge of JavaScript.
Role required: script_include_admin

1. Create a script include with the name <tablename>DisplayFilter.
   The script section contains one function with the same name as the script include.

2. Use your function to set the global variable `answer` to either true (show the filters and breadcrumbs) or false (hide them.)
   The following example restricts filters and breadcrumbs on the Incident table to users with any role. Be sure that the name of the script matches the function name exactly, including case.

   ```javascript
   var incidentDisplayFilter = Class.create();
   incidentDisplayFilter.prototype = {
       type: 'incidentDisplayFilter',
       initialize: function() {
       },
       incidentDisplayFilter: function() {
           var answer;
           if (gs.hasRole()) {
               answer = true;
           } else {
               answer = false;
           }
           return answer;
       }
   };  
   ```

3. Optional: To exclude a specific role from having access to filters and breadcrumbs, make the following change.

   ```javascript
   var incidentDisplayFilter = Class.create();
   incidentDisplayFilter.prototype = {
       type: 'incidentDisplayFilter',
       initialize: function() {
       },
       incidentDisplayFilter: function() {
           var answer;
           if (gs.hasRole() && !gs.hasRole('newrole')) {
               answer = true;
           } else {
               answer = false;
           }
           return answer;
       }
   };  
   ```

   Users with the role `newRole` do not have access to filters and breadcrumbs.

4. Optional: To let all users use filters and breadcrumbs on the Incident table, make the following change to your script.

   ```javascript
   var incidentDisplayFilter = Class.create();
   incidentDisplayFilter.prototype = {
       type: 'incidentDisplayFilter',
   ```
initialize: function() {
},
incidentDisplayFilter: function() {
var answer = true;
return answer;
};

5. Optional: To modify filter and breadcrumb access for another table, create a script include using the name of that table instead of Incident.

Increase the allowed number of breadcrumb entries

You can add a property to allow for a larger number of breadcrumb entries in the filter.

Role required: admin

1. Enter `sys_properties.list` in the Navigation filter.
   The entire list of properties in the System Properties [sys_properties] table appears.
2. Verify that the property does not exist by searching for `glide.ui.breadcrumb_max_entries`.
3. Click New.
4. Complete the form as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>glide.ui.breadcrumb_max_entries</td>
</tr>
<tr>
<td>Type</td>
<td>integer</td>
</tr>
<tr>
<td>Value</td>
<td>The number of breadcrumb entries you want to appear in the filter, for example, 15. The default number is 10.</td>
</tr>
</tbody>
</table>

5. To verify this property, go to any table and use the filter modifier `is one of` to search for any number of items. The number of entries you entered in the Value field displays before ending in a [...].

Breadcrumb entries

Enable a hierarchical list

You can enable hierarchical lists to make data from related lists directly accessible from within a v2 list.

Role required: personalize_control

Hierarchical lists enable a user to view the contents of the related lists of a record without leaving the record list form.
**Note:** You cannot enable a hierarchical list view for an embedded list. Hierarchical lists are not supported in List v3, even if they are enabled.

1. Right-click any column header, and select **Configure > List Control** from the context menu.
2. Select the **Hierarchical lists** check box in the List Control dialog box and then click **Submit** or **Update**.
3. Click the arrow for a record number to display the related lists for the record.
**Use list controls in hierarchical lists**

By default, no related list tabs are visible in a hierarchical list and only a single related list is displayed at a time. The column headers are hidden by default.

Role required: none

Note: Hierarchical lists are not supported in List v3.

1. To select a different related list, click the link in the list title.
2. Select a list from the menu.

If the related list is empty, the hierarchical list indicates that there are no records to display.

The platform remembers this preference and displays the last selected related list for each table when you open another hierarchical list within that table.
3. To display column headers in the related list, click the show/hide headers icon in the upper right corner of the hierarchical list.

The platform remembers this preference and opens all hierarchical lists with column headers enabled until the headers are hidden.

Context ranking

Context ranking allows a user to sort a collection of records preferentially, that is, independently of the attributes of those records.

For example, a Customer Support manager can organize a list of incidents in the order in which a technician should work on the tasks. Creating such an arbitrary list with a list filter is not possible.

Activate context ranking

If you have the admin role, you can activate the Context Ranking plugin (com.glide.sorting). This plugin activates related plugins if they are not already active.

Role required: admin

1. Navigate to System Applications > All Available Applications > All.

2. Find the Context Ranking plugin (com.glide.sorting) using the filter criteria and search bar.

You can search for the plugin by its name or ID. If you cannot find a plugin, you might have to request it from ServiceNow personnel. For more information, see Request a plugin.
3. Click **Install**, and then in the Activate Plugin dialog box, click **Activate**.

**Note:** When domain separation and delegated admin are enabled in an instance, the administrative user must be in the **global** domain. Otherwise, the following error appears: Application installation is unavailable because another operation is running: Plugin Activation for <plugin name>.

---

### Create a ranking definition

Enable context ranking for a related list by creating a ranking definition.

Role required: admin

1. Navigate to **System Definition > Ranking Definitions**.
2. Click **New**.
3. Enter a **Name** for the ranking definition.
4. In the **Record table** field, select the table for which ranking is enabled.
   This is the table of the records in the ranked related list. For example, to enable ranking for a related list of incidents in the Problem form, select the Incident [incident] table.
5. In the **Context column** field, select the reference column providing the context in which ranking is to be performed.
   The context in this case is the form in which the related list appears and not a table name. For example, a related list with a **Record table** of Incident [incident] can have several contexts, including the **Problem** form or a **Configuration item** form.
6. Complete the relationship-based fields if the ranking is to be performed on a related list that is defined by a relationship.
   - **Relationship table**: select the table forming the other side of the relationship. In the case of the ranking definition for Product stories in scrum, you might use the Product Model [cmdb_model] table.
   - **Relationship column**: select the column from the relationship table to compare with the context column. To avoid adding a related list of user stories to the Product Model [cmdb_model] table, you might use the **Sys ID** column, which defines a subclass of the Product Model table (cmdb_model.sys_id).
7. In the **Attributes** field, enter attributes to change and restrict the contents of the Rank dialog box, as appropriate.
   - **visible_columns**: a semi-colon separated list of columns to be displayed in the Rank dialog box. If not specified, the Rank dialog box uses the default view of the related list you selected in the **Record table** field.
   - **extra_conditions**: an encoded query to restrict the records shown in the Rank dialog box. For example, the query `extra_conditions=^state!=7` displays all incidents whose state is not **Closed**. If not specified, the Rank dialog box shows all records for the relationship.
8. Click **Submit**.
   The index is generated automatically. The system completes these read-only fields:
   - Index column
   - Rank ui action
   - Context menu item

**Note:** After you submit a ranking definition, only the **Attributes** field can be edited. If additional changes are required, delete the record and create a new one with the revised settings.
The system does not generate indexes for ranking definitions inserted into the database by an update set. To use a ranking definition inserted by an update set, you must generate the indexes manually. To generate indexes, open the Ranking Definition form, and click **Generate Indexes**.

### Rank a list

After you create a ranking definition for a table, related lists based on that table and context include options for ranking the list and displaying the list by rank.

Role required: none
You can set the preferential order of records.

1. Click the **Rank** button in the related list to reorder the records.

The Rank dialog box appears, allowing you to sort the records in any order.
2. Click and drag the move icon ( ) to change the position of a record.

**Note:** Administrators can define which columns appear in the Rank dialog box in the Attributes field of the Ranking Definition form.
**Apply a new sort order to a list**

You can apply a new sort order to the records in a list.

Role required: none

1. Open the context menu from the list title and select **Sort by rank**.

![Sort by rank](image)

2. To remove the ranking and return to the original order of the list, click the label in any column that contains data.

**Scrum ranking definitions**

Ranking definitions for user stories are part of the SDLC (scrum process) application.

These ranking definitions enable scrum users with the proper roles to rank related lists of stories in these tables:

- Product stories: Application Model [cmdb_application_product_model] table
- Release stories: Release [rm_release] table
- Sprint stories: Sprint [rm_sprint] table

Users can rank stories in the scrum planning board by priority. Story lists ranked in the planning board appear in the new order in product, release, and sprint forms. Stories ranked in one of these scrum forms changes the order in the planning board.

Story points for each story are listed in a ranked view, which is useful for prioritizing stories.
Ranking story points

Rank stories in a related list

The Context Ranking feature enables all scrum users to manually sort a related list of stories by priority.

A product owner or release planner uses this tool to establish the order in which he or she wants the stories worked. Stories ranked in a related list (in the Product, Release, and Sprint forms) appear in the same order in the planning board when the appropriate backlog is displayed. Conversely, stories ranked in the planning board appear in that order when viewed in the related list in the form. Users can switch the view in a Stories related list from ranked to any sort order without changing the ranking in the planning board.

1. In the Stories related list, click Rank.
   A dialog box appears, allowing you to arrange the stories in any order, such as by priority.
2. Click and drag each story into position using the move icon to the left of the story number.

3. When you are done, click the X in the upper right corner to close the list.
   The Stories related list is not sorted by your ranking initially.
4. To view the related list in its ranked order, open the context menu from the related list and select **Sort by rank**.

![Sort by rank menu](image)

5. To return the sort order of the list to an unranked state, click once in the heading of any column that contains data.

The system uses this ranked list to display the appropriate backlog in the planning board. For example, if you rank stories in the **Stories** related list in the Release form, the release backlog in the planning board uses the same ranking to display the stories. Conversely, scrum masters, product owners, and release planners can create a new ranking order for the **Stories** related list by rearranging the list of stories in the planning board.

### Customize List v2 context menus

You can customize the content and behavior of List v2 context menus.

Role required: admin

For example, you might add an option to the list column heading menu for a specific table. You might also want to change the roles required to access a global context menu option.

**Note:** This functionality is not supported in List v3. Context menu options created this way do not appear in v3 lists. Administrators can create UI actions instead.

1. Navigate to **System UI > UI Context Menus**.
2. Click **New**.
3. Complete the form.

**Context menu form fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>Select the table to which this context menu option is attached. The base system menu items are attached to the Global [global] table, which applies the context menu option to all lists for all tables. If you specify a particular table, the option is available only on context menus in lists from that table. <strong>Note:</strong> The list shows only tables and database views that are in the same scope as the context menu.</td>
</tr>
<tr>
<td>Menu</td>
<td>Select the list context menu in which this option appears.</td>
</tr>
<tr>
<td>• List title menus</td>
<td></td>
</tr>
<tr>
<td>• Column headings</td>
<td></td>
</tr>
<tr>
<td>• List row menu</td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>Select the type of menu option to create:</td>
</tr>
<tr>
<td>• <strong>Action</strong>: A menu option that performs an immediate action.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Menu</strong>: Creates a parent menu that can display a submenu.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Separator</strong>: Draws a line between groups of options on a menu. Menus do not display separator lines next to one another or at the bottom of a menu. If a condition that removes options for a role forces two separators together, one of the separators is removed from the view.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Label</strong>: Create an unlinked label for a menu or section of a menu.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Dynamic actions</strong>: Menu options dynamically created, such as the available views or user filters that can only be generated at the time the list is displayed.</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Enter the label for the action as it will appear in the menu.</td>
</tr>
<tr>
<td>Parent</td>
<td>If this action is part of a submenu, type the name of the parent menu item. For example, in the base system, <strong>Configure</strong> is a parent.</td>
</tr>
<tr>
<td>Order</td>
<td>Assign an order number to this item, menu, or separator to specify where in the menu it appears.</td>
</tr>
<tr>
<td>Active</td>
<td>Enable or disable this context menu item. Only active items are shown in the context menu.</td>
</tr>
<tr>
<td>Run onShow script</td>
<td>Select this check box to display the <strong>onShow script</strong> field.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Condition</td>
<td>Create the conditions under which this menu option appears. For example, define the role that has permission to see this item.</td>
</tr>
<tr>
<td>Action script</td>
<td>The action script runs when someone selects the context menu option. For more information, see Action script for List v2 context menus.</td>
</tr>
<tr>
<td>Dynamic actions script</td>
<td>The dynamic actions script populates the context menu with dynamic options, such as filters or views. For more information, see Dynamic actions script for List v2 context menus.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>onShow script</td>
<td>The onShow script runs before the context menu is displayed, to determine which options appear in the context menu. For more information, see onShow script for List v2 context menus.</td>
</tr>
</tbody>
</table>
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
4. Click **Submit**.

**Action script for List v2 context menus**

The **Action script** field, on the Context Menu form, defines a script. The script runs when someone selects the context menu option.

This script is client-side and runs in the user’s browser. The following JavaScript variables are available to the Action script when it is executed.

**Action script variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>g_list</td>
<td>GlideList2 against which the script runs.</td>
</tr>
<tr>
<td>g_fieldName</td>
<td>Name of the field against which the context menu runs.</td>
</tr>
<tr>
<td>g_fieldLabel</td>
<td>Label of the field against which the context menu runs.</td>
</tr>
<tr>
<td>g_sysId</td>
<td>The sys_id of the row or form against which the script runs.</td>
</tr>
</tbody>
</table>

The base system uses the following code in an action script to refresh the platform view.

```javascript
    g_list.refresh(1);
```

Another example is the use of these variables in a list header menu to sort a list by the selected field in descending order (z to a).

```javascript
    g_list.sortDescending(g_fieldName);
```

**Dynamic actions script for List v2 context menus**

The **Dynamic actions script** field, on the Context Menu form, defines a script. The script populates a list context menu with dynamic options, such as filters or views.

The following JavaScript variables are available to the dynamic actions script when it is executed.

**Dynamic actions script variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>g_tableName</td>
<td>Name of the current table.</td>
</tr>
<tr>
<td>g_listId</td>
<td>ID of the list for which the context menu is built.</td>
</tr>
<tr>
<td>g_itemName</td>
<td>Name defined in the UI context menu record.</td>
</tr>
<tr>
<td>g_itemOrder</td>
<td>Order defined in the UI context menu record. Use this variable to pass the value of the Order field to the dynamic actions script.</td>
</tr>
<tr>
<td>g_contextMenu.addAction(item_id, label, script_string, order)</td>
<td>Add options to the context menu and select the order in which they appear.</td>
</tr>
</tbody>
</table>
The following example displays a list title menu item that controls the number of records per page in the list view.

```javascript
g_contextMenu.addAction('50', g_itemName, 'showRowsPerPage("50");', g_itemOrder);
```

**Note:** The action script for this item must define the `showRowsPerPage` function so that when selecting this menu item, that function is called with an argument of 50.

### onShow script for List v2 context menus

The **onShow script** field defines a script that runs before the context menu is displayed to determine which options appear in the context menu.

Use this script to change the menu items on the list header menu based on the current field column. The following JavaScript variables are available to the **onShow** script when it is executed:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>g_menu</td>
<td>Context menu to be displayed.</td>
</tr>
<tr>
<td>g_item</td>
<td>Current context menu item.</td>
</tr>
<tr>
<td>g_list</td>
<td>GlideList2 against which the script runs.</td>
</tr>
<tr>
<td>g_fieldName</td>
<td>Name of the field against which the context menu runs.</td>
</tr>
<tr>
<td>g_fieldLabel</td>
<td>Label of the field against which the context menu runs.</td>
</tr>
<tr>
<td>g_sysId</td>
<td>The sys_id of the row or form against which the script runs.</td>
</tr>
</tbody>
</table>

An example of an **onShow** script is one that determines when to enable or disable the **Ungroup** option in a list column heading menu based on whether the list is grouped or not.

```javascript
if (g_list.getGroupBy()) {
    // list is grouped so enable to Ungroup menu item
    g_menu.setEnabled(g_item);
} else {
    // list is not grouped, so disable the Ungroup menu item
    g_menu.setDisabled(g_item);
}
```

### List v3 administration

List v3 is no longer available for new deployments. If you are already using List v3, you can continue to do so. There are several aspects of list administration that are specific to List v3.

#### Supported browsers for List v3

List v3 is supported on recent versions of most major browsers.

- The latest public release of Firefox or Firefox ESR
- The latest public release of Chrome
- Safari version 9.1 and later
- The latest public release of Microsoft Edge
• Internet Explorer version 11
  • Edge mode is supported.
  • Compatibility mode is not supported.
  • Setting Security Mode to High (via the Internet Options > Security tab) is not supported.

**Internet Explorer**

**Important:** Due to significant performance issues, ServiceNow recommends that customers migrate away from Internet Explorer 11. For more information, refer to KB0683275.

• Internet Explorer 11 is susceptible to memory leaks, which may impact performance, especially in Windows 7.
• In Jakarta and later, Internet Explorer versions prior to IE11 are no longer supported.
• Compatibility mode is not supported.
• Setting the Security Mode to High (in the Internet Options > Security tab) is not supported.

**List v3 compatibility**

Certain conditions prevent lists from displaying in List v3.

A list loads in List v2 under the following circumstances.

• List v3 is disabled globally. Disabling List v3 globally overrides all other conditions. By default, List v3 is enabled globally when the List v3 plugin is activated.
• The list is a related list and List v3 has not been enabled for related lists. By default, List v3 is disabled for related lists.
• The associated list control has any of the following fields set to true:
  • Disable list v3 (by default, this field is set to false for most tables)
  • Hierarchical lists
  • List edit insert row
• All the associated client-side list UI actions that are active have the List v3 Compatible field set to false. Client-side list UI actions have the Client and List action fields set to true.

**Note:** Embedded lists and list reports are not supported in List v3 and always display in List v2.

**Debug List v3 compatibility**

If a list displays in v2 when List v3 is enabled globally, you can debug compatibility and fix the issue quickly.

Role required: admin

The debug List v3 compatibility icon (🔧) appears in the title bar of v2 lists.

**Note:** Administrators can configure which roles can see the icon by modifying the glide.ui.list_v3.debug_compatibility.roles property. For more information, see Properties for List v3.

1. Click the debug List v3 compatibility icon.
   A compatibility checklist opens. Each applicable condition and its compatibility status, pass (√) or fail (❌), is listed. If there are client-side UI actions that are not compatible, each one is listed by name.
2. Point to the pass or fail icon to view an explanation of the condition criteria.
3. For failed conditions, click the link to navigate directly to the source of the problem.

**Properties for List v3**

Defines the properties that are available for List v3.

List v3 uses the following properties. These properties do not impact List v2 functionality.

**Note:** To open the System Property [sys_properties] table, enter `sys_properties.list` in the navigation filter.

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
</table>
| glide.ui.admin_import_xml_roles | Determines which user roles are required to access the Import XML option in the list title menu. When the value is blank, no role is required.  
  - Type: string  
  - Default value: admin  
  - Location: System Property [sys_properties] table |
| glide.ui.list.allow_search_box  | Allows the search box to display even if the filter controls are restricted.  
  - Type: true | false  
  - Default value: false  
  - Location: Add to the System Property [sys_properties] table |
<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.ui.list_v3.append_module_title</td>
<td>Appends the name of the module from which a list was accessed to the list title when enabled. For example, if you open the Incident list by navigating to <strong>Incident &gt; All</strong>, the list title is <strong>Incidents (All)</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: true</td>
</tr>
<tr>
<td></td>
<td>• Location: System Property [sys_properties] table</td>
</tr>
<tr>
<td>glide.ui.list_v3.chart_limit</td>
<td>Sets the maximum number of groups to display in list grouping charts.</td>
</tr>
<tr>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 12</td>
</tr>
<tr>
<td></td>
<td>• Location: Add to the System Property [sys_properties] table</td>
</tr>
<tr>
<td>glide.ui.list_v3.debug_compatibility.roles</td>
<td>Determines which user roles are required to access the debug List v3 compatibility icon, which appears in the title bar of v2 lists when List v3 is enabled globally. When the value is blank, no role is required.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: admin</td>
</tr>
<tr>
<td></td>
<td>• Location: Add to the System Property [sys_properties] table</td>
</tr>
<tr>
<td>Enable List v3</td>
<td>Determines whether List v3 is enabled globally. Additional conditions may prevent incompatible lists from loading in List v3, even when this property is enabled.</td>
</tr>
<tr>
<td>glide.ui.list_v3.enable</td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: true</td>
</tr>
<tr>
<td></td>
<td>• Location: <strong>System Properties &gt; List v3</strong></td>
</tr>
<tr>
<td></td>
<td>• Learn more: Disable List v3 globally</td>
</tr>
<tr>
<td>glide.ui.list_v3.limit_chart_data</td>
<td>Determines whether list grouping charts display the <strong>Other</strong> category when the number of groups exceeds the value set in the <strong>glide.ui.list_v3.chart_limit</strong> property.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: true</td>
</tr>
<tr>
<td></td>
<td>• Location: Add to the System Property [sys_properties] table</td>
</tr>
<tr>
<td>Property</td>
<td>Usage</td>
</tr>
<tr>
<td>----------</td>
<td>-------</td>
</tr>
</tbody>
</table>
| Enable List v3 for Related Lists on Forms<br>glide.ui.list_v3.related_list | Determines whether List v3 is enabled for related lists. The **glide.ui.list_v3.enable** property must be set to **true** to enable List v3 for related lists.  
  - Type: choice list  
  - Default value: enable_async_v2  
  - Available values:  
    - off: Disables List v3 for related lists. List v2 is used.  
    - enable_v3: Enables List v3 for related lists.  
    - enable_async_v2: Uses list v2 for related lists, but loads them asynchronously. When form tabs are enabled, only the lists on the visible tab are loaded.  
  - Location: **System Properties > List v3**  
  - Learn more: **Enable List v3 for related lists** |
| Enables real-time record updates on List v3 (Note: this may impact system performance)<br>glide.ui16.live_lists.enabled | Determines whether live updates are enabled for v3 lists. When live updates are enabled, record updates appear in real time, without the need to refresh the list manually. In Jakarta and after, live lists are enabled by default.  
  - Type: true | false  
  - Default value: true  
  - Location: **System Properties > List v3** |
| Allow related list query conditions to be added through the filter<br>glide.ui.list.related_list_search_filter | Determines whether the related list conditions builder is enabled for List v3 list views. The **glide.ui.list_v3.enable** property must be set to **true** to enable the related list conditions builder.  
  - Type: true | false  
  - Default value: true  
  - Location: **System Properties > List v3**  
  - Learn more: **Add related list conditions Add related list conditions** |
| Lowering the value of glide.ui.list.record_watcher_throttle property may impact system performance.<br>glide.ui.list.record_watcher_throttle | Time (ms) to wait between reacting to record watch events  
  - Type: integer  
  - Default value: 30000  
  - Location: **System Properties > List v3** |
| glide.ui.list_v3.enable_live_related_lists | Determines whether live updates are enabled for v3 related lists. When live updates are enabled, record updates appear in real time, without the need to refresh the list manually.  
  - Type: true | false  
  - Default value: true  
  - Location: System property [sys_properties] table |
Configure available related tables for the related list query

You can configure which related list tables are available to users in the related list query. The related list query is only available in List v3.

Role required: admin

Related Lists Conditions choice list

Users only see the related tables that they are authorized to view. The administrator can add a system property for any table and specify which related tables to exclude for everyone from the choice list.

1. To configure the related tables to exclude, add a new system property with the following field values.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>&lt;table&gt;.related_list_query.blacklist</td>
</tr>
<tr>
<td>Type</td>
<td>string</td>
</tr>
<tr>
<td>Value</td>
<td>comma-separated list of tables to exclude from the choice list.</td>
</tr>
<tr>
<td></td>
<td>Example: task_sla.task, task_ci.task</td>
</tr>
</tbody>
</table>

2. Click Submit.

Add this system property for every table for which you want to exclude related table choices.
Configure list calculations in List v3

In List v3, you can configure list calculations for columns, which calculate column totals, minimums, maximums, and averages.

Role required: personalize_list

You can configure list calculations for multiple columns in the same list. List calculations apply only to the view of the list in which they are configured. All users can see configured list calculations.

Note: List calculations are available in list reports, but the configuration instructions are different because list reports display v2 lists. For more information, see Configure list calculations in List v2.

1. In a list, click the list title menu icon and select **List Calculations**.

   The List Calculations window opens. It lists all columns that are visible in the current list.
2. Select the check box for one or more of the following calculation options for any column. You can only select calculation options that are available for a given column.
   - Average (not available for string, date, or date/time fields)
   - Minimum
   - Maximum
   - Total (not available for string, date, or date/time fields)

   A calculation preview appears by the check box.

3. To remove all list calculations, click **Clear Calculations**.

4. Close the List Calculations window.

   The calculations appear at the bottom of the list for each configured column.

---

### Enable List v3 for related lists

List v3 is disabled for related lists by default. You can enable List v3 for related lists by editing a property.

**Incompatible** related lists display in List v2, even when List v3 is enabled for related lists. If a form contains both v2 and v3 related lists, the differences in behavior and appearance may impact user experience. Evaluate how much work is required to ensure that each form displays related lists of the same version.

Role required: admin

1. Navigate to **System Properties > List v3**.
2. Locate the property called **Enable List v3 for Related Lists on Forms (glide.ui.list_v3.related_list)** and select **Enable V3** from the list.
3. Click **Save**.

   Assuming that List v3 is enabled globally, all compatible related lists display in List v3.

---

### Disable List v3 globally

You can disable List v3 globally by editing a property.

Role required: admin

When you disable List v3 globally, all lists load in List v2 for all users.

1. Navigate to **System Properties > List v3**.
2. Locate the property called **Enable List v3 (glide.ui.list_v3.enable)** and clear the check box.

3. Click **Save**.

**Disable List v3 for a specific list**

You can configure a specific list view to display v2 lists, even when the List v3 feature is enabled.

Role required: personalize_control
For example, you may need to disable List v3 for a list until you can train everyone who uses the application about the new location of the controls.

1. Navigate to the list for which you want to disable List v3.
2. Click the list title menu icon ( ).
3. Select Configure > List Control.
   The List Control form appears.
4. Select the Disable list v3 check box.
5. Click Update.

**Form configuration**

Form configuration involves changing the form layout and the related list layout. The form layout changes what appears on the form and the related list layout changes which related lists appear at the bottom of the form.

You change aspects of a form such as showing or hiding fields, embedding lists, and adding sections and annotations. This video highlights form layout and design.

**Using the form designer**

Administrators or users with the personalize_form role can use the form design feature to quickly create new or change existing form views.

With form design, you can accomplish the same tasks that you can with form layout in a graphical tool called the form designer. You can also access field properties and add information from macros or previously scripted UI elements.

Form design is an alternative to configuring forms that combines several configuration options into one tool. It is available by default for new instances and requires UI16 or UI15. Administrators who upgrade from a previous version must activate the Form Designer (com.glide.ui.ng.fd) plugin to use the feature.
Parts of the UI form design interface

The page header

The page header displays the current table and view being designed. Each form is tied to a unique table and view combination. For example, there can only be one form for the incident table default view. Select a different view to modify different form layouts for a table.
The field navigator

The field navigator allows you to manage fields on the form. It contains the following elements:

- **Filter**: Allows text search on the currently selected tab.
- **Fields**: Displays a list of existing fields you can add to the current form.
- **Field Types**: Displays a list of field types you can add to the current form. Adding a field type to the form layout creates fields in the selected table when the form layout is saved.
Field properties are accessed by clicking the gear icon that appears when you point to a field in the form layout.
The form layout displays a separate cell for each field, section, annotation, UI element, and related list that is on the form. Each cell has an identifying label and a handle icon to aid in selecting and moving it. The location of the cell in the form layout represents its relative position on the form. Only fields visible on the form layout are displayed on a form.
Form layout
Show or hide fields with the form designer

You can move fields to and from the form workspace to display the fields on the form.

Role required: personalize_form

Use the filter to quickly find fields in the field navigator.

1. Navigate to the form designer.
2. From the list of fields in the Field Navigator, select the field you want to display from the list of available fields.
3. Drag the field to the form layout.
4. Drag the field to the location you want it to be on the form.
5. To remove a field from the form layout, select the field and click the Remove this field (X) button beside the field label.
6. Click Save.

Add a form annotation with the form designer

Use annotations to provide instructions or additional information about fields on a form.

Role required: personalize_form

1. Navigate to the form designer.
2. Click the Field Types tab.
3. Select the Annotations field type.
4. Drag the annotation to the appropriate location on the form.
5. Point to the Annotations field and click the gear icon to open Properties dialog box.
6. In the Properties dialog box, enter a value for Annotation Text. You can use HTML tags to format the annotation text.
7. Click Save.

Add a new section with the form designer

Move sections to and from the form layout to display or remove the sections on the form.

Role required: personalize_form

Sections can have a one- or two-column layout.

By default, the first section on a form is always a read-only section displaying the label of the table. You cannot remove this section.

1. Navigate to the form designer.
2. Select an existing section.
3. Click the (+) button beside the section label to add a section.
4. Enter a label for the section.
5. Drag sections to reorder them.
   The label for the first section on the form designer is displayed as the form title.
6. To delete a section, click the (x) button beside the section label.
7. Click **Save**.

The following GIF shows how you would use form designer to add and then delete a form section.
Add a formatter with the form designer

Use formatters to add information from macros or previously scripted UI elements to a form.

Formatters are used to add information from macros or previously scripted UI elements to a form.

1. Navigate to the form designer.
2. Click the **Fields** tab.
3. In the filter, enter the string `Format`.
4. Select the formatter you want to add to the form.
5. Drag the formatter to the location you want it to be on the form.
6. Click **Save**.

Add a new field with the form designer

You can add a field to a form and the associated table.

Role required: personalize_form

Adding a field creates a dictionary entry for the new column in the current table. You can create a custom table and then use the form designer to add fields to the form.

Use the filter to quickly find field types in the field navigator.

1. Navigate to the form designer.
2. Click the **Field Types** tab.
3. Select the cell for the field type to create.
4. Drag the field type to the location you want it to be on the form.
5. Enter a label for the field.
6. Optional: Point to a field in the form design area and click the gear icon to access properties.
7. Click **Save**.

Configuring the form layout

Administrators or users with the personalize_form role can configure the form and related list layout.

Show or hide fields on a form

Configure form layout to change what appears on the form. You can perform tasks like changing what fields are visible, embedding lists, and adding sections and annotations.

Role required: personalize_form

1. Navigate to a form.
2. Click the context menu icon
   ( )
   and select **Configure > Form Layout**.
3. Using the slushbucket, select the fields and the order in which you want them to appear. Available items that appear in green followed by a plus (+) sign represent related tables. To access fields on these tables, use dot-walking.

In UI16, Form Layout is not responsible for the order of the Additional Comments and Work Notes fields. For more information on how to determine the order of these fields, see Customize activities.
4. Click **Save**.

**Warning:** Do not add the same field to more than one section of a form unless the field displays read-only data. Having two or more instances of an editable field can cause data loss and prevent the proper functioning of UI and data policies.

Through form configuration, you can also add new fields to the form, which creates columns to the table that underlies the form. See [Add and customize a field in a table](#) for more information.

### Add a related list to a form

You can configure related lists to appear on forms and in hierarchical lists.

Role required: personalize_form

Related lists display records in another table that have a relationship with the current record.

1. Open the form.
2. Click the form context menu icon and select **Configure > Related Lists**.
3. Using the slushbucket, select the related list to display on the form.
4. Click **Save**.
   
   Related lists appear at the bottom of the form.

### Add an annotation to a form

Highlight form elements by displaying blocks of colored text or separators between form elements.

Role required: personalize_form

1. Navigate to a form.
2. Click the context menu icon and select **Configure > Form Layout**.
3. Under **Form view and section**, select a section.
4. In the Available list, double-click *Annotation* to move it to the Selected list.

The Annotation Details section appears.

5. Place it above the field to annotate.
6. In Annotation Details, select the type of annotation. The available types of annotations include **Info Box Blue**, **Info Box Red**, **Line Separator** (any text you add appears beneath the line), **Section Details**, **Section Separator**, and **Text**.
7. Select either Plain Text or HTML for the data type and enter the annotation in the text box. All valid HTML tags are supported.

   For example, select the Text annotation type, the HTML data type, and enter `<span style="color:red">Select the primary location:</span>`. The text appears red on the form.

8. Click Save.

### Toggle annotations

Users can toggle annotations on a form in UI16 and UI15. The `glide.ui.show_annotations` user preference controls the visibility of annotations for each user.

1. Navigate to a form.
2. Perform the appropriate action for your version of the UI.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>UI16</td>
<td>Click the more options icon (omore_icon) to see the annotations icon. The icon is light gray and cannot be toggled when no annotations are available.</td>
</tr>
<tr>
<td>UI15</td>
<td>Click the annotation toggle icon (?_icon) to show or hide annotations.</td>
</tr>
</tbody>
</table>

### Create a form section

Create sections on forms to help group related fields together.

Role required: form_admin

Users can expand or collapse form sections to show or hide the fields they need. If you have tabs enabled, each form section appears on a separate tab. The default Change Request form is an example of a form with multiple sections as shown in the following image.
Change Request form sections

1. Right-click the form header and select **Configure > Form Layout**.
2. In the **Form view and section** area below the slushbucket, click **New** in the **Section** list.
3. In the **Section caption** field, give the new section a title, then click **OK**.
4. Select a form section name and click the up or down arrow to change the section order.

**Note:** The caption for the first section on the form becomes the form title.

5. Add fields to the new section using the slushbucket.
6. Click **Save** when you are finished.

The new section appears on the form with the fields you selected. If you do not add any fields to a section, the section stays empty.

If you want to delete the form section later, do the following:

a. Navigate to **System UI > Form Sections**.

b. Filter for the table that contains the section you want to delete. For example, the Incident table. The name of the form section to be deleted is displayed in the **Caption** field.

c. Select the check box beside the form section to delete, and then select **Delete** from the **Actions on selected rows** menu.

d. Click **OK** to confirm the deletion.

### Move form splits

Change the place where fields split on a form by moving the split section indicators in a slushbucket.

Role required: admin

1. Navigate to a form.
2. Click the context menu icon

   ![Context Menu Icon]

   and select **Configure > Form Layout**.
3. Move any of the following split section indicators:
   - `- begin_split -`
   - `- split -`
   - `- end_split -`
4. Click **Save**.
Display tabbed forms

Tabbed forms offer a useful way to make forms and related lists take up less space by reducing the scrolling that must be done to navigate the form.
Tabbed forms
Form sections and related lists are tabbed separately, each with their own tab line. A user always sees the first form section. All sections after that can be tabbed. Tabs are enabled by default for new instances.

Tabbed forms are enabled by default for new instances. A system user preference with the name `tabbed.forms` specifies whether the tabbed UI is used by default for all users. Users can change this preference as described in this procedure.

1. Click the gear icon in the banner frame.
2. Perform the appropriate action for your version of the UI:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UI16</td>
<td>Select the Forms tab and enable Tabbed forms.</td>
</tr>
<tr>
<td>UI15</td>
<td>Enable Tabbed forms.</td>
</tr>
</tbody>
</table>

An option is enabled when the switch appears green and is toggled to the right.

**Embed a list within a form**

You can embed lists within a form. When a list is embedded in a form, any changes made to the contents of the list are saved when the form is saved.

Role required: personalize_form

This allows the embedded list to be treated just like another element on the form. In addition, users can create records in the list view. After a row is added to the list, double-click any cell in the list to edit its value. You can add the same lists to a form as embedded lists or as related lists, depending on the path selected in the context menu.

You can also modify embedded list controls, such as the name of the related list and the roles required to create records in the embedded list.

1. Select a record from the list.
2. Right-click the form header and select **Configure > Form Layout**.
   The slushbucket shows the available fields and the lists that can be embedded in the form. Lists appear in red at the bottom of the **Available** list.
3. Select a list and move it to the **Selected** column.
4. Use the up and down arrow buttons to position the list in the form.
5. Click **Save**.

Lists adjust to fit the frames of the adjacent fields.
Configure customer updates indicator

You can configure the indicator for customer updates, which are changes that update sets, scripts, service catalog items, and other configuration tables track.

Role required: admin

The customer updates indicator icon (💬) may appear on the header of forms that have customer updates. Clicking the customer updates indicator opens the update set records for the item.

You can configure this indicator to appear for all or for specific administrators using the `owned_by_indicator.form` user preference.

1. Navigate to User Administration > User Preferences.
2. Perform one of the following actions.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the indicator for all administrators</td>
<td>Set the <code>owned_by_indicator.form</code> preference to true.</td>
</tr>
</tbody>
</table>
| Enable the indicator for an individual administrator | a. Make sure the `owned_by_indicator.form` system user preference is set to false.  
|                                             | b. Create a user preference with the following values: |
|                                             | • Name: `owned_by_indicator.form`  
|                                             | • User: Select the administrator for which to enable the preference.  
|                                             | • Value: true |

Add a chart to a form

Add a chart to a form to show your users graphical data related to the form. For example, you could show an incident SLA-related chart on the Incident form so your users can see how well service level agreements are being met.

Role required: personalize_form

Note: The following report types are not supported on forms: List, Pivot, Multilevel Pivot, Calendar, and Single Score.
Chart on a form

1. Navigate to **System UI > Forms**.
2. Select the form you want to configure.
3. Click the context menu icon
   
   ![Chart icon]

   and select **Configure > Form Layout**.
4. Using the slushbucket, select *Chart*.
5. Enter a **Label** in the chart details.
6. Click **Save** to return to the form.
7. Click **Configure chart**.
8. Select a chart in the **Report** field and configure other options as desired.
9. Click **Update**.
Form administration

Administrators can configure several settings that control form functionality.

Form personalization
Control how users configure forms. You can also change the role that is necessary to configure a form and disable the form configurations that specific users already made.

See Administering form personalization for instructions.

Form annotations
Choose the types of annotations that are available on forms and save localized versions of form annotations.

See Administering form annotations for instructions.

Attachments
Control several aspects of form attachments, such as attachment size, allowed file extensions, and the roles that are allowed to attach files.

See Administering attachments for instructions.

Formatters
Create and edit formatters, such as the activity formatter, which displays information on the form that is not a field in the record. You can also configure formatter settings such as the maximum number of formatter entries.

See Formatters for more information.

Form templates
Create templates that automatically populate form fields based on settings you configure.

See Form templates for more information.

UI actions
Add buttons, links, and context menu items on forms to the UI more interactive, customizable, and specific to user activities.

See UI actions for more information.

UI policies
Configure the policies that dynamically change information on a form.

See Create a UI policy for more information.

Other advanced options
Configure advanced form features, such as form focus, form splits, and derived fields.

See Advanced form configuration for instructions.

Administering form personalization

Administrators can configure several aspects of form personalization, which allows users to customize the layout for any form view.

Administrators can manage this function using the following options.

• Activate or deactivate form personalization globally.
• Control user access to form personalization based on roles.
• Manage the personalized forms of users.

**Note:** Personalizing a form in this way modifies the form for you only. To make changes to a form that are visible to all users, you must configure the form.

### Activate form personalization

Form personalization is activated for new instances. To activate form personalization for upgraded instances, an administrator must activate the Form Personalization (com.glide.ui.personalize_form) plugin.

**Role required:** admin

1. Navigate to **System Applications > All Available Applications > All**.
2. Find the Form Personalization (com.glide.ui.personalize_form) plugin using the filter criteria and search bar. You can search for the plugin by its name or ID. If you cannot find a plugin, you might have to request it from ServiceNow personnel. For more information, see [Request a plugin](#).
3. Click **Install**, and then in the Activate Plugin dialog box, click **Activate**.

**Note:** When domain separation and delegated admin are enabled in an instance, the administrative user must be in the **global** domain. Otherwise, the following error appears: Application installation is unavailable because another operation is running: Plugin Activation for <plugin name>.

### Change form personalization role requirements

By default, the itil role is required to personalize forms, but you can change this requirement with a system property.

**Role required:** admin

1. Enter `sys_properties.list` in the navigation filter.
2. Locate the `glide.ui.personalize_form.role` property in the System Properties list.
3. In the **Value** field, specify the roles that can access form personalization.

### Manage personalized forms

When a user personalizes a form, the system stores the customizations as a user preference record. You can view and manage the user preferences.

**Role required:** admin

1. Navigate to **User Administration > User Preferences**.
2. Filter the list by `[Name] [contains] [personalize]`.
   There is a user preference for each form view each user personalizes. The name format combines the word personalize with the name of the table and the name of the view. For example, if a user personalizes the default view of the Asset [alm_asset] form, the user preference is called `personalize alm_asset_default`.
3. Delete a user preference to remove the customizations for the user.

### Disable form personalization

If you do not want your users to customize forms, you can disable form personalization.

**Role required:** admin
Activating the Personalize Forms plugin sets the `glide.ui.personalize_form` property to true. You can disable form personalization.

1. Enter `sys_properties.list` in the navigation filter.
2. Locate the `glide.ui.personalize_form` property in the System Properties list.
3. Set the Value field to `false`.

**Administering form annotations**

Form annotations are additional pieces of information on a form, such as a line or paragraph of text. Use form annotations to provide on-screen instructions to your users.

Form annotations are enabled by default in the base system. To disable them, set the `glide.ui.form_annotations` system property to false.

**Support multiple languages for a form annotation**

You can store multiple translations of form annotation text.

Role required: admin

To support multiple languages, use message records to translate annotation text.

1. Navigate to System UI > Messages.
2. Create a message record for each language you support.
3. On the Message form, set the Key field to a unique identifier for the annotation text. The annotation text is a good key. The key must be the same for each translation message for the annotation.
4. Select the appropriate Language.
5. In the Message field, enter the translated annotation text.
6. Edit the form annotation and reference the message key with a `gs.getMessage` call.
   
   For example, if the message key is `Message key text`, enter `$(gs.getMessage("Message key text"))` in the form annotation.

**Administer form annotation types**

You can define the form annotation types to control their appearance.

Role required: admin

1. Navigate to System UI > Form Annotation Types.
2. Set the Active field to `false` for any types you do not want to use.
3. Click New to add a type.

**Administering attachments**

Administrators can configure system properties for how files are uploaded and attached to records. Uploading, viewing, and deleting file attachments triggers a single event that can be used for notifications or in scripts.

**Attachment tables**

When you store an attachment to any table, a record is created in the Attachment [sys_attachment] table that contains attachment metadata. The file data is stored in the Attachment Document [sys_attachment_doc] table, in 4k chunks.
For example, if you attach a 12k file called `My_attachment.pdf`, then there is an Attachment entry with three related Attachment Document entries.

To learn how to upload attachments to records, see Add and manage attachments.

Activity stream thumbnail scaling

The `glide.ui.activity_stream.scale_images` property scales large images down and creates thumbnails for the activity stream view of the images. This property is active by default. It applies to images retroactively, so any attachments included in an activity stream in the past also see the effects.

- Maximum dimensions for thumbnails using this property are 525 pixels width by 350 pixels height. The system favors the pixel height first, so you can end up with images that are wider than 525 pixels.
- Attaching image files over 5 MB can create an out of memory error and cause the instance to restart. An out of memory error and restart occur when the system generates the thumbnail when you attach a new image. The error and restart can also occur the first time you load existing images on a record.
- The administrator can add the `com.glide.attachment.max_get_size` system property to control the maximum image scaling dimensions.

Enter the following information into the `[sys_properties.list]` table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>com.glide.attachment.max_get_size</td>
</tr>
<tr>
<td>Type</td>
<td>integer</td>
</tr>
<tr>
<td>Value</td>
<td>5242880</td>
</tr>
</tbody>
</table>

The value field represents the size in bytes.

- The base system value is 5242880 bytes (5 MB). You can change the value as necessary.
- With this property set, images that are larger than 5 MB are not scaled and the system creates a link instead. Images smaller than 5 MB are scaled down.

Configure the max image size property for Activity Streams

When attaching an image in an Activity Stream, the system controls the maximum size of the image. Use the `com.glide.attachment.max_get_size` property to control the maximum image scaling dimensions.

Attachment events and logging

A script action or notification can process attachment events. Only one event is created when action is taken on a record with attachments, even when the record has multiple attachments. The following events are provided.

Only one event is created when action is taken on a record with attachments, even when the record has multiple attachments. The following events are provided.

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>attachment.read</td>
<td>An attachment has been read or downloaded.</td>
</tr>
</tbody>
</table>
### Event Logging

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>attachment.uploaded</td>
<td>An attachment has been uploaded. If multiple attachments are uploaded to a record at one time, only one event is created.</td>
</tr>
<tr>
<td>attachment.deleted</td>
<td>An attachment has been deleted. This event is also triggered when the record containing the attachment is deleted. If a record is deleted that contains multiple attachments, a separate event is triggered for each attachment in the deleted record.</td>
</tr>
<tr>
<td>attachment.renamed</td>
<td>An attachment has been renamed.</td>
</tr>
</tbody>
</table>

### Attachment logging

When an attachment is downloaded, the `attachment.read` event record is written, and you can do something with this event. For example, you can record when and by whom certain attachments are downloaded. For this functionality, `current` is a `sys_attachment` record, and the event record uses the following parameters:

- **parm1**: File name
- **parm2**: Table name

### Debug attachment indexing

To change debugging options for attachment indexing, add these system properties.

- **glide.ts.index.attachment.debug**: When the value is set to `true`, enables log messages for exceptions that occur when indexing attachments (default is `false`).
  
  You can leave this property enabled during normal operations to capture stack trace information about any exceptions.

- **glide.ts.index.attachment.list_terms.debug**: When the value is set to `true`, logs all indexed terms when an attachment is indexed (default is `false`).

  [Recommended] For optimal performance, set this property to `false` during normal operations. Only enable this property when you are actively debugging an issue.

**Note**: To learn more about the properties that affect attachments processing, see Attachments (instance security hardening) in Instance Security Hardening Settings.

### Configure attachment system properties

You can disable the drag-and-drop feature. (Users can still upload attachments by browsing to the file.) You can also limit the attachment file size, restrict who can upload attachments, and restrict what file extensions can be uploaded.

Role required: admin

**Note**: To learn more about the properties that affect attachments processing, see Attachments (instance security hardening) in Instance Security Hardening Settings.

1. To disable the drag-and-drop features, navigate to **System Properties > UI Properties**.
2. Clear the check box for the **Allow attachment drag and drop in supported HTML5 browsers** property.
3. Click **Save**.

**Limit attachment file size**

You can specify the maximum size allowable for attachments to avoid issues with the user's active session on the instance. The maximum attachment size for email attachments is configured separately.

Role required: Admin.

Note: The maximum attachment size for email attachments is configured separately.

1. Navigate to **System Properties > Security**.
2. Enter a value in the **Maximum file attachment size in megabytes** property.
   The system only allows attachment sizes up to 1 GB. By default, this field is blank. If you leave this field blank, the system uses the default maximum limit of 1 GB.
3. Click **Save**.

**Require a role to attach files**

You can restrict who can upload attachments.

Role required: Admin.

1. Navigate to **System Properties > Security**.
2. In the **Attachment limits and behavior** section, locate the **List of roles (comma-separated) that can create attachments** property (**glide.attachment.role**).
3. Enter one or more roles separated by commas.
   Only roles listed in this property are able to upload attachments to a record. If no roles are entered, then all roles can upload attachments.
4. Click **Save**.

**Restrict attachment file extensions**

The **glide.attachment.extensions** property restricts the file extensions that users can upload as attachments.

Role required: Admin.

Use this property to improve security by preventing users from uploading harmful files, such as viruses, as attachments. Also, this capability can prevent the use of incompatible filetypes. For example, Internet Explorer does not support icons in .png format. This property does not restrict files based on the actual file type, but only based on the extension.

1. Navigate to **System Properties > Security**.
2. In the **Attachment limits and behavior** section, locate the **List of file extensions (comma-separated) that can be attached to documents via the attachment dialog** property.
3. Enter the file extensions and click **Save**.
   If no extensions are specified, then all extensions are allowed. However, if any extensions are specified, all unlisted extensions are restricted. Listed extensions should not include the dot (.) prefix or spaces after commas. For example, enter xls,xlsx,doc,docx.

**Disable attachments on a table**

You can prevent users from adding attachments to records on a specific table.
Role required: admin

1. Open a record in the table.
2. Right-click the form header and select **Configure > Dictionary**.
3. In the list of dictionary entries, select the first record in the list (the record with no **Column name** entry).
4. Add **no_attachment** to the **Attributes** field, separated by commas from any existing attributes.
   
   See **Dictionary attributes** for more information.

## Index attachments on a table

You can enable attachment indexing for a table so text searches can return matches from the record and its file attachments.

Role required: admin

By default, attachment indexing is enabled for the Knowledge Base. Enabling attachment indexing causes the platform to reindex the selected table, its parent table, and any children of the parent table. For large tables, such as the Task table, reindexing can take several hours and slows down the system until complete. Reindexing is best performed during non-peak times.

1. Open a record in the table.
2. Right-click the form header and select **Configure > Dictionary**.
3. On the Dictionary Entries list, open the first record.
   
   The first record has the record type **Collection** and doesn't have any entry for **Column name**.
4. Open the **Attributes** tab, and then click **New**.
5. On the form, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute</td>
<td>Select Attachment index.</td>
</tr>
<tr>
<td>Value</td>
<td>Enter true.</td>
</tr>
</tbody>
</table>

**Note:** The attachment indexing attribute only applies to the tables on which you explicitly add it. It does not cascade to child tables. For example, indexing attachments on the Task table does not index attachments on the Incident table. Not all file types are supported for attachment indexing. For a list of supported file types, see Zing can include attachments in search results.

6. Click **Submit**.
7. On the Dictionary Entry form, click the **Generate Text Index** related link.
8. On the confirmation window, click **OK**.

In the confirmation window, you can select to have the system send you an email notification after the text indexing is complete.

The indexing process begins. When it is complete, attachments can be searched on that table.

### Hide the attachment [view] link

Users can open an attachment by clicking either the file name or the **[view]** link. The **[view]** link opens the file from within the browser, which executes JavaScript code as part of the attachment. You can hide the **[view]** link. Users can still view attachments by clicking the file name.

Role required: Admin.

1. Add the `glide.ui.disable_attachment_view` and `glide.ui.attachment_popup` properties.
   
   For instructions on adding properties to the platform, see [Add a system property](#).

2. For the `glide.ui.disable_attachment_view` property, set the **Type** to **true/false** and set the **Value** to **true**.

3. For the `glide.ui.attachment_popup` property, set the **Type** to **true/false** and set the **Value** to **false**.

4. To return to the default behavior (enable the link), set the `glide.ui.attachment_popup` property **Value** to **true**.

### Configure attachment icons

You can configure the icon that appears beside an attachment of a particular file type.

Role required: Admin

1. Determine the path of the image file. If desired, upload a new image.

2. Navigate to **System UI > Attachment Icon Rules**.

3. Open an existing rule or click **New** to create a new rule.
4. Enter the rule details.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select icon by</td>
<td>Select MIME Type or File Extension.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>If a file type has an icon specified by MIME Type and a different icon specified by File Extension, the MIME Type icon takes precedence.</td>
</tr>
</tbody>
</table>

| MIME type        | If Select icon by is MIME Type, enter the MIME type and subtype to associate with the icon, separated by a slash (example: application/pdf). |
| File extension   | If Select icon by is File Extension, enter the file extension to associate with the icon beginning with the period (example: .pdf). |
| Icon             | Enter the path to the icon image file (example: images/icons/attach_pdf.gifx) |

5. Click Submit or Update.

**Formatters**

A formatter is a form element used to display information that is not a field in the record. Add formatters to a form by configuring the form.

**Examples of formatters in the base platform**

<table>
<thead>
<tr>
<th>Formatter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity formatter</td>
<td>Displays the list of activities, or history, on a task form.</td>
</tr>
<tr>
<td>Process flowformatter</td>
<td>Displays the different stages in a linear process flow across the top of a record.</td>
</tr>
<tr>
<td>Parent breadcrumbs formatter</td>
<td>Provides breadcrumbs to show the parent or parents of the current task.</td>
</tr>
<tr>
<td>Approval summarizer formatter</td>
<td>Displays dynamic summary information about the request being approved.</td>
</tr>
<tr>
<td>CI relations formatter</td>
<td>Displays on the CI form a toolbar for viewing the relationships between the current CI and related CIs.</td>
</tr>
</tbody>
</table>

**Note:** Formatter elements cannot be exported to PDF. When exporting PDF data from a form, any formatter elements added to the form are not displayed in the PDF output.

To create a custom formatter, create a UI macro to define content for the formatter, then create a formatter that refers to the UI macro. You can then add the formatter to a form.

**Create a UI macro for a formatter**

Create a UI macro to define the content that the formatter displays.

This functionality requires knowledge of Jelly script.
Role required: ui_macro_admin

1. Navigate to System UI > UI Macros.
2. Click New.
3. Complete the form.
4. In the XML script field, enter Jelly script to define the content to be displayed by the formatter.

**Note:** The UI Macro for the formatter represents a row in the UI. It must begin and end with `<TR></TR>` tags.

```xml
<?xml version = "1.0" encoding = "utf-8" ?>
<j:jelly trim="false" xmlns:j="jelly:core" xmlns:g="glide" xmlns:j2="null" xmlns:g2="null">
<tr>
<td colspan="2">
Here  is some descriptive text  for the Priority field.
</td>
</tr>
</j:jelly>
```

This Jelly script is reproduced below in plain text that you can copy into the Macro form as a basis for your macro script.
5. Click **Submit**.

### Create a formatter and add it to a form

Create the formatter after creating the UI macro that defines the content.

Role required: admin

With the UI macro in place, create the formatter that references it, and add it to the form.

1. Navigate to **System UI > Formatters**.
2. Click **New**.
3. In the **Name** field, enter a descriptive name for the formatter.
4. In the **Formatter** field, enter the name of the UI macro with `.xml` appended to it.
5. In the **Table** field, select the table in which the formatter will be used.
6. In the **Type** field, select **Formatter**.
7. Click **Submit**.
8. To add the formatter to a form, configure the form.

   The formatter appears on the form according to your selections.

### Activity formatter

The activity formatter provides an easy way to track items not saved with a field in the record, for example, journal fields like comments and work notes.

The activity formatter is enabled by default on the Task [task] table and other tables that extend the Task table, such as the Incident [incident] table. It is also enabled on the Approvals [sysapproval_approver] table.

You can filter the content that appears on the activity formatter and participate in the record feeds on the record. You can create an activity formatter for any form and configure properties that control what fields appear in the formatter. The number next to activities indicates the number of entries in the record feed. The number updates when users use the filter.

Activity type and a time stamp display in the top of each entry.

In UI16, the activity formatter shows updates in real time so you can see the latest information without refreshing the form. User presence enables you to see when other users are entering comments.
Activities: 5

**System Administrator**

Field Changes • 2017-06-28 16:21:04

**Don Goodlife**

Server out of memory

Additional comments • 2017-06-07 17:18:48

**Don Goodlife**

Added an attachment

Additional comments • 2017-06-07 17:18:48

**Don Goodlife**

Moved to Issue 'Doing' from 'To Do'

Work notes • 2017-06-07 17:18:48

**Don Goodlife**

Field Changes • 2017-06-07 17:18:48

Assigned to: David Loo
Impact: High
Incident state: In Progress
Opened by: Don Goodlife
Priority: Critical
Create an activity formatter

You can create an activity formatter for any audited table.

Role required: admin

1. Navigate to **System UI > Formatters**.
2. Click **New**.
3. Enter a name for the formatter, such as **Activities (task)**.
4. Select a **Table**.
5. Enter **activity.xml** in the **Formatter** field.
6. Leave the **Type** as **Formatter**.
7. Click **Submit**.

**Note:** You can create more than one activity formatter for a table, however, the system does not allow you to add more than one activity formatter to a form.

Add the new activity formatter to forms as needed.

Add the activity formatter to a form

Add an activity formatter to any form to track journal fields on the form.

Role required: personalize_form

1. Verify that the table associated with the form is audited.
2. Configure the form layout to add **Activities (filtered)**.

**Note:** In UI16, you cannot place another field in between a journal field and the activities formatter. The Activity Stream is built to keep journal fields stacked on top of the activity formatter.

**Note:** Field styles are not applied to comments and work notes fields used with the activity formatter. Styles for these fields can be set using the `glide.ui.activity_stream.style.comments` and `glide.ui.activity_stream.style.work_notes` system properties located on the `sys_properties` table.

Enable the Live Feed-Activity toggle

The Live Feed-Activity toggle allows users to switch between the activity feed and the document feed for a record.

Role required: admin

Use live feed to interact with other users on a record by posting messages and adding attachments to the feed. Use the activity formatter to see an overall summary of activity for the record.
Live Feed/Activity toggle

- The `glide.ui.show_live_feed_activity` property is enabled. Navigate to Collaborate > Feed Administration > Properties and enable the Toggle the display of the live feed tab in the activity formatter option.

1. Verify that the live feed and record feed plugins are active.
2. View the form to ensure that the activity formatter is visible. If not, configure the form to add it.
3. Set the `live_feed` dictionary attribute to true on the form.
   This action adds live feed to the activity formatter.
4. Complete the following steps to enable the system property.
   a) Navigate to Collaborate > Feed Administration > Properties.
   b) Enable the Toggle the display of the live feed tab in the activity formatter option (`glide.ui.show_live_feed_activity` property).

Customize activities

You can customize which fields appear in the activity formatter. You can add or remove fields from the list of activities that users can select when they open the activity filter.

Role required: personalize_form and personalize_list
Customize the fields that appear in the activity filter

**Note:** In the UI15 interface, the number of updates to each field was shown in parentheses to the left of each field. This has been removed in UI16.

1. Perform the appropriate action for your version of the UI:

<table>
<thead>
<tr>
<th>UI version</th>
<th>Action</th>
</tr>
</thead>
</table>
| UI16       | a. Click the activity filter icon ( ¶ ).  
|            | b. At the bottom of the list, click **Configure available fields**. |
| UI15       | Right-click the **Activity** header and select **Configure Activities**. |
2. In the slushbucket, select the desired fields in the **Available** column and move them to the **Selected** column. The activities appear in alphabetical order, regardless of the order in the **Selected** column.

   **Note:** In UI16, **Configure available fields** is responsible for the order of the Additional Comments and Work Notes fields.

3. Click **Save** to add them to the activity formatter and the filter.

Administrators can also modify the system property **Incident activity formatter fields(glide.ui.incident_activity.fields)**. Access this property through **System Properties > UI Properties**. The system automatically synchronizes the values in the system property and the selections you made.

**Configure roles for viewing emails in the activity formatter**

The system property **glide.ui.activity.email_roles** enables you to control which roles can see emails in the activity formatter.

Role required: admin

In the activity formatter, users see activity only for fields they have permission to read. For example, self-service users might see the activity formatter on the self-service view of the Incident form, but they do not see work notes, unless security rules have been customized to allow this.

If the **Sent/Received Emails** field is included in the activities list, all users see all emails. No determination is made whether an end user, for example, should see an email containing work notes. Configure this property to restrict this capability to specified roles.

   **Note:** Email does not appear as an activity until it is sent. If email properties are not configured for outbound delivery, the message can be found by navigating to **System Mailboxes > Outbox**.

1. Navigate to **System Properties > UI Properties**.
2. Locate the property labeled **List of roles (comma separated) that can view emails in the Activity Formatter when "Sent/Received Emails" are included.**
3. Add roles to the property, separated by commas.
   These are the only roles that can see email in the activity formatter. All other roles are prevented from seeing email. If no roles are listed, all users can see email. The itil role is on the list by default.
4. Click **Save**.

**Configure the max activity size property**

Use the **glide.max_activity_size** property to increase the amount of content that can be visible in the Activity Formatter.

Role required: admin

The default size for an activity is 100 * 1024, which causes large amounts of content to be hidden in the Activity Formatter. You can change the default value by adding the **glide.max_activity_size** property.

1. Type **sys_properties.list** in the Application Navigator.
2. Click **New** and enter the following values.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>glide.max_activity_size</td>
</tr>
<tr>
<td>Type</td>
<td>integer</td>
</tr>
</tbody>
</table>
Configure email reply for the activity formatter in UI16

The `glide.ui16.emailStreamResponseActions` system property determines whether a user can reply to email using the email reply button in the activity stream in UI16.

1. In the navigation filter, type `sys_properties.list`.
2. Add the following system property. For more information on adding a system property, see Add a system property.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>glide.ui16.emailStreamResponseActions</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Add the email reply button to the activity stream.</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>true</td>
</tr>
<tr>
<td><strong>Value</strong></td>
<td>Set the value to <strong>true</strong>. The default value if this property is not configured is false.</td>
</tr>
</tbody>
</table>

3. Click Submit.

Configure email reply for the activity formatter in UI15

The `email_reply` UI macro creates an email reply button in the activity stream in UI15. This UI macro can be deactivated to hide the button.

1. Navigate to **System UI > UI Macros**.
2. Open the `email_reply` UI macro record.
3. Check the check box in the **Active** field to enable the email reply button, or uncheck the field to disable it.
4. Click Submit

Process flow formatter

The process flow formatter provides a graphical summary of the stages in a process. The formatter is typically shown at the top of forms that are part of a process.

Each record on the Flow Formatter [sys_process_flow] table represents a process stage and can have a different condition applied to it. When specified conditions are fulfilled, the formatter highlights the current stage and places a check mark next to all previous stages.

These examples show a workflow in the UI15 and UI16 interfaces.

**UI15 process flow for an incident**
UI16 process flow for a change request

When any formatter stages are defined for a table, they appear on the form associated with that table in the order specified, assuming the formatter has been added to the form.

Activate the process flow formatter

You can activate the Process Flow Formatter plugin.

Role required: admin

1. Navigate to System Applications > All Available Applications > All.
2. Find the plugin using the filter criteria and search bar.
   - You can search for the plugin by its name or ID. If you cannot find a plugin, you might have to request it from ServiceNow personnel. For more information, see Request a plugin.
3. Click Install, and then in the Activate Plugin dialog box, click Activate.

Note: When domain separation and delegated admin are enabled in an instance, the administrative user must be in the global domain. Otherwise, the following error appears: Application installation is unavailable because another operation is running: Plugin Activation for <plugin name>.

Create a process flow formatter

You can create a process flow formatter stage.

Role required: admin

2. Click New.
3. Complete the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>Select a table for this process flow formatter.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter a name to identify the formatter.</td>
</tr>
<tr>
<td>Label</td>
<td>Enter the name to be displayed in the form configuration slushbucket.</td>
</tr>
</tbody>
</table>
Field | Description
---|---
Active | Select the check box to ensure that the formatter stage is active. When the check box is cleared, the formatter stage does not appear in the flow display.
Order | Enter a number to indicate where in the process flow the formatter will be displayed. Formatters are arranged with the lowest number on the left and the highest number on the right.
Condition | Use the condition builder to set the conditions under which the formatter is highlighted as current. Any field available in the condition builder, such as SLA or Impact, can be used to trigger a process flow stage.
Description | Describe the process flow formatter. This description does not appear on the actual formatter.

4. Repeat as necessary for each stage.

**Parent breadcrumbs formatter**

The parent breadcrumbs formatter on the Task table provides breadcrumbs that show the parent or parents of the current task. This formatter can be used also on any table that extends Task.

Role required: personalize_form

To add the parent breadcrumbs formatter to a form, configure the form and add **Parent Breadcrumbs** to the desired location. The breadcrumbs show only six levels of parents. If more levels exist, the breadcrumbs display an ellipsis ("...").

The **Parent** reference field also has to contain a value for the breadcrumbs to appear. You may need to configure the form to contain the **Parent** field as well.
Customize the parent breadcrumbs formatter

You can customize the parent breadcrumbs formatter to control what breadcrumbs appear.

**Role required:** admin

1. Navigate to **System UI > Formatters**.
2. Select **Parent Breadcrumbs**.
3. Click **View UI Macro for this Formatter** to view or modify the underlying formatter.

By default, the breadcrumb uses the default display field, `gr.getDisplayValue()`, as the link in the breadcrumb. To customize this, add the following line, replacing the `fieldName` parameter with the desired field name (not the field label):

```javascript
pc.setLabelField("fieldName")
```

If a user points to a breadcrumb, the short description for that record appears as a hint by default. To display alternate hints for the breadcrumb, add the following line, replacing the `fieldName` parameter with the desired field name (not the field label):

```javascript
pc.setTitleField("fieldName")
```

Be sure to add these lines in the proper location, as shown in the following example:

```javascript
//parent crumb functions - script include
var pc = new ParentCrumbs(now_GR);
pc.setLabelField("short_description");

//override the default display field to be used for label
pc.setTitleField("number");

//override default short_description hover text
var crumbs = pc.getCrumbs();
```

Use the parent breadcrumbs formatter on non-Task tables

The parent breadcrumbs formatter can be used on non-Task tables as long as the table has a reference to itself through a field called **parent**.

Role required: admin

To make the formatter available for a different table, duplicate the formatter used by the Task table:

1. Navigate to **System UI > Formatters**.
2. Select **Parent Breadcrumbs**.
3. Set the **Table** field to the appropriate table.
4. Right-click the form header and choose **Insert**.
5. Add the new formatter to the appropriate form.

Approval summarizer formatter

The approval summarizer formatter creates the summary at the bottom of an approval form.
The approval summarizer displays different information depending on what is being approved, such as a change request or a service catalog request. Following are two examples.
### Summary of Item being approved

#### Change Request

<table>
<thead>
<tr>
<th>Number</th>
<th>CHG0000001</th>
<th>Requested by</th>
<th>David Loo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affected CI</td>
<td>Sales Force Automation</td>
<td>Type</td>
<td>Normal</td>
</tr>
<tr>
<td>Planned start date</td>
<td>2016-07-27 16:00:00</td>
<td>Risk</td>
<td>High</td>
</tr>
<tr>
<td>Planned end date</td>
<td>2016-07-27 18:00:00</td>
<td>Impact</td>
<td>3 - Low</td>
</tr>
<tr>
<td>Short description</td>
<td>Rollback Oracle Version</td>
<td>Description</td>
<td>Performance of the Siebel SFA software has been severely degraded since the upgrade performed this weekend. We moved to an unsupported Oracle DB version. Need to rollback the Oracle Instance to a supported version.</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved. ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Summary of a catalog request

The **Reject** button allows the approver to deny one or more requested items in a multi-item request, before approving the overall request. If a requested item is denied, the workflow for that item never starts. The approver can then choose to **Accept** the item.

**Note:** When the overall request is approved, you must ensure this **Reject** button is hidden. If this button is used after request approval, the requested item workflow is canceled, leaving the stage in an inconsistent state. Similarly, the **Accept** button on requested items should only appear before the overall request is approved or rejected.

Override a formatter with macros

The system uses formatters to handle complex rendering of specific form elements.

Role required: `ui_macro_admin`

Examples of form elements rendered by formatters in the base platform are:

- Activity formatter: Displays the list of activities, or history, on a task form.
- Process flow formatter: Displays the different stages in a linear process flow across the top of a record.
- Task parent breadcrumbs formatter: Provides breadcrumbs to show the parent or parents of the current task.
- Approval summarizer formatter: Displays dynamic summary information about the element being approved.

A UI macro can override formatters provided in the base system.

1. Navigate to **System UI > UI Macros**.
2. Click **New**.
3. In the **Name** field, enter the same name as the formatter you want to override, but omit the `.xml` extension.
4. Complete the remaining fields on the form.
5. Click Submit.

This example shows the form that defines the existing approval summarizer formatter:

Here is the form for the UI macro that overrides the approval summarizer formatter:

Limit the number of activity stream entries

You can set a system property to limit the number of entries allowed in an activity stream.

Role required: admin

1. Enter `sys_properties.list` in the Navigation filter.
2. Search for the property `glide.history.max_entries`.
3. Edit the Value property to set the maximum number of entries that users can view in an activity stream.

Note: New entries do not count towards the max number until the form is refreshed.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>glide.history.max_entries</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Description</td>
<td>Maximum number of entries allowed to display in an activity stream. The default number is 250. New entries do not count towards the max number until the form is refreshed.</td>
</tr>
<tr>
<td>Type</td>
<td>integer</td>
</tr>
<tr>
<td>Default value</td>
<td>250</td>
</tr>
</tbody>
</table>

### Form templates

Templates simplify the process of submitting new records by populating fields automatically.

To use a template, populate the most-used fields for a specific table, save it as a template, and then make the template accessible to your users. Users can manually apply a template when creating records, or an administrator can define scripts to apply templates automatically.

Create templates for the forms that you use frequently, such as incident, problem, and change. There is no limit to the number of templates that you can create or access, but having many templates for each form makes the templates more complex to manage.

You can create table-level access controls to restrict template creation. When applied, a user creating a new record from a template must satisfy the save_as_template access control for every field modified by the template.

### Automatically applied templates

You can make a template that automatically applies to new, user-created records on a specific table. To create this kind of template, set the template name to match the name of the table to which the template applies.

For example, imagine you want to apply a template automatically when a user creates a record on the Windows Server [cmdb_ci_win_server] table. Set the Name field to cmdb_ci_win_server and the Table field to Windows Server [cmdb_ci_win_server] on the Template form.

Automatic templates are always global. They do not honor the User and Group fields on the Template form. Automatic templates do not apply to records created by the system, such as those records generated by business rules, UI actions, or workflows.

### Create a template using the Template form

Create a template record for any table to automatically populate certain fields.

Role required: admin

1. Navigate to System Definition > Templates.
2. Click New.
3. On the form, fill in the fields.

#### Template form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of this template.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Table</strong></td>
<td>Table that this template applies to. Select <strong>Global</strong> to make the template available for use with all tables.</td>
</tr>
<tr>
<td><strong>Note</strong>:</td>
<td>The table list shows only the tables and database views that are in the same scope as the template.</td>
</tr>
<tr>
<td><strong>Active</strong></td>
<td>Option for making the template available for use. A template must be active to be used.</td>
</tr>
<tr>
<td><strong>User</strong></td>
<td>User who can configure and apply the template. If you define a user, no other users can see the template unless you select the <strong>Global</strong> option.</td>
</tr>
<tr>
<td><strong>Group</strong></td>
<td>Group whose members can configure and apply the template. If you define a group, no other groups can see the template unless you select the <strong>Global</strong> option.</td>
</tr>
<tr>
<td><strong>Global</strong></td>
<td>Option for allowing any user who can access the templates to view and apply this template.</td>
</tr>
<tr>
<td><strong>Short description</strong></td>
<td>Description of the template.</td>
</tr>
<tr>
<td><strong>Note</strong>:</td>
<td>Adding content to this field does not add that content to the <strong>Short description</strong> field of the forms that use this template.</td>
</tr>
<tr>
<td><strong>Template</strong></td>
<td>Content that automatically populates records that are based on this template. Select a field from the specified table in the left column and then enter the data to automatically populate in the right column.</td>
</tr>
<tr>
<td><strong>Note</strong>:</td>
<td>Even though you can select dot-walked fields in the template, they do not apply to fields that are on the form.</td>
</tr>
<tr>
<td><strong>Link element</strong></td>
<td>Template that links a child table with the template for the parent table. In the template for the child table, set the value to the field that references the parent table. After you set the value, the child template is explicitly linked to the parent table.</td>
</tr>
<tr>
<td><strong>Note</strong>:</td>
<td>This field does not appear by default. Configure the template form to add the field.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

See **Application scope**.

**Create templates for related task records**

Administrators can create a template for a Task table record that also creates one or more related records in the child Task table.

Role required: admin

Administrators must understand the parent-child relationships between Task tables. For example, the Change Task table is a child of the Change table and the Incident Task table is a child of the Incident table.
Note: Child templates can only be applied automatically if you first apply the parent template from a module.

1. From the parent Task table template, configure the form layout to add these fields.
   - Next Related Child Template
   - Next Related Template
   - Link element

2. Create a template for the parent Task table.
   For example, create this template for the Change table.

   **Sample Change template**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Add server to network</td>
</tr>
<tr>
<td>Table</td>
<td>Change [change_request]</td>
</tr>
<tr>
<td>Short description</td>
<td>Set up a server on the network</td>
</tr>
<tr>
<td>Template</td>
<td>• [Short description][Set up server on the network]</td>
</tr>
<tr>
<td></td>
<td>• [Category][Hardware]</td>
</tr>
<tr>
<td></td>
<td>• [Assignment group][Hardware]</td>
</tr>
</tbody>
</table>

3. Create a template for the first related task.
   For example, create this template for the Change Task table.

   **First sample Change Task template**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Order server</td>
</tr>
<tr>
<td>Table</td>
<td>Change Task [change_task]</td>
</tr>
<tr>
<td>Short description</td>
<td>Order server hardware</td>
</tr>
<tr>
<td>Template</td>
<td>• [Short description][Order server hardware]</td>
</tr>
<tr>
<td></td>
<td>• [Assignment group][Hardware]</td>
</tr>
<tr>
<td>Link element</td>
<td>Change request</td>
</tr>
</tbody>
</table>

4. Create a template for each additional related task.
   For example, create one additional template for the Change Task table.

   **Second sample Change Task template**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Install server on network</td>
</tr>
<tr>
<td>Table</td>
<td>Change Task [change_task]</td>
</tr>
<tr>
<td>Short description</td>
<td>Install server on network</td>
</tr>
<tr>
<td>Field</td>
<td>Value</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>Template</td>
<td>• [Short description] [Install server on network]</td>
</tr>
<tr>
<td></td>
<td>• [Assignment group] [Hardware]</td>
</tr>
<tr>
<td>Link element</td>
<td>Change request</td>
</tr>
</tbody>
</table>
5. From the parent Task table template, set **Next Related Child Template** to the first related child task.

For example, in the Add server to network template, select **Order server** in the **Next Related Child Template** field.
6. For each child related task, set **Next Related Template** to the next related task template. For example, in the Order server template, select **Install server on network** in the **Next Related Template** field.

**Note:** The last related task template does not have a value for **Next Related Template**. For example, the **Install server on network** template does not have a value in **Next Related Template**.
Create a module for the parent Task table template so that child templates can be applied to related task records. For example, create a module for Add server to network.

Create a template by saving a form

Save a populated form as a template.

Toggle the template bar so it is visible on forms.

Role required: none

1. Navigate to a form.
2. Complete the form as it should appear when a user applies the template.
3. In the template bar, click the plus icon (+).

4. Enter a descriptive name to make it easy for a user to select the correct template.

5. Make any additional changes as needed.

6. Click Save.
Create records based on a template

You can create and schedule a scheduled job to create records based on a template. For example, you can regularly create a populated task record to perform a weekly backup.

Role required: admin

1. Navigate to System Definition > Templates.
2. Select a template record.
3. Click Schedule.
   The Scheduled Entity Generation form appears.
4. In the Run choice list, select how frequently to create a record.
5. Complete the schedule information.
6. Click Submit.

Create a module for a template

You can create a module to open a form with pre-populated template data.

Role required: admin

Child templates are only applied if the parent template is applied from a module. Child templates are not applied by applying a template to a new form.

1. Perform the appropriate action for your version of the UI:

<table>
<thead>
<tr>
<th>UI16</th>
<th>Point to the application menu, such as Self-Service, and click the edit application (pencil) icon.</th>
</tr>
</thead>
<tbody>
<tr>
<td>UI15</td>
<td>Right-click an application menu and select Edit Application Menu.</td>
</tr>
</tbody>
</table>

2. In the Modules related list, click New.
3. Fill in the Title and Order fields as appropriate.
4. In the Link Type form section, in the table field, select the table you want to create the form in.
5. In the Link Type field, select New Record.
6. In the Arguments field, enter `<table>.do?sys_id=-1&sysparm_template=<templatename>`
   The `<table>` is the name of the table you selected for the table field, for example incident. The `<templatename>` is the name of the template you want to use to pre-populate the form, for example Incident call type.
7. Click Submit.
8. Refresh the application navigator to view the new module.

Template bar

Use the template bar to apply, edit, and create templates.

The template bar appears at the bottom of the form. Click a template, which appears in blue text, to apply them to the form. Use the buttons to the right to add, edit, and access the complete list of templates.
Template Bar in UI16

**Template Bar Elements**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Templates</td>
<td>Available templates appear in blue text on the template bar. Click a template to apply it to the form.</td>
</tr>
<tr>
<td>All Templates button</td>
<td>Toggles the All Templates window.</td>
</tr>
<tr>
<td>Create New Template button</td>
<td>Displays the Create New Template window.</td>
</tr>
<tr>
<td>Element</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>All Templates popup</td>
<td>This window displays when the <strong>All Templates</strong> button is selected. The window displays a filterable list of all available templates. Click the <strong>Edit</strong> button to the left of any template to edit that template.</td>
</tr>
<tr>
<td>Disable Template Bar button</td>
<td>Enables or disables the template bar. To display the bar, see <strong>Toggle the template bar</strong>.</td>
</tr>
</tbody>
</table>

**Toggle the template bar**

The template bar appears at the bottom of forms. It provides shortcuts to apply, edit, and create templates.

Role required: none

You can toggle the template bar, which hides or shows it for all forms. The template bar is shown by default.

1. Navigate to a form.
2. Do the appropriate action for your version of the UI.

   **UI16**
   
   a. Click the more options icon in the form header.
   
   b. Select **Toggle Template Bar**.

   **UI15**
   
   a. Right-click the form header.
b. Select **Toggle Template Bar**.

The template bar is hidden or shown.

**Scripted templates**

You can apply an active template to a record using JavaScript.

**Apply a template to current**

To apply a template, use the `applyTemplate` method.

```javascript
current.applyTemplate("<templatename>");
```

**Apply a template to a GlideRecord**

To apply the template to a record other than current, change current to a GlideRecord variable. When using a GlideRecord variable, you may need to initialize it after declaring the variable.

```javascript
var rec1 = new GlideRecord("incident");
rec1.initialize();
rec1.applyTemplate("my_incident_template");
```

**Apply a template from a UI action**

The following script demonstrates a possible customization to the **Create Change** UI action on the Problem form. After you add this script to the UI action, a user can select the UI action to create a change record with information from both the problem record and the change template.

```javascript
var change = new GlideRecord("change_request");
change.initialize();
change.short_description = current.short_description;
change.description = current.u_details;
change.cmdb_ci = current.u_service;
change.priority = current.priority;
change.requested_by = current.caller_id;
change.assignments_group.setDisplayValue('Change & Release');
change.u_status = 'New';
change.parent = current.number;
change.applyTemplate("standard_rfc");
change.rfc = change.insert();
change.comments = 'Change ' + change.number + ' created.';
var mySysID = current.update();
gs.addInfoMessage("Change " + change.number + " created");
action.setRedirectURL(change);
action.setReturnURL(current);
```
Script a template with child templates

When using `applyTemplate` with a template that has one or more child templates, the system creates the parent record before applying the child templates. This behavior ensures that any references or dot-walked fields from the child record to the parent have a valid target.

For example, if a template for the Change Request table has a child template for the Change Task table, applying the Change Request template inserts a Change Request record into the database. It assigns this record as the Change request for the Change Task record, then applies the child template to the Change Task record.

UI actions

UI actions include the buttons, links, and context menu items on forms and lists. Configure UI actions to make the UI more interactive, customized, and specific to user activities.

Administrators and users with the `ui_action_admin` role can define UI actions.

UI action controls

You can create a UI action to provide any of these controls:

- A button on a form.
- A context menu item on a form that appears when you open the form context menu or right-click the form header.
- A related link in a form.
- A button in the banner on top of a list.
- A button at the bottom of a list.
- A context menu item on a list that appears when you open the list context menu or right-click the list header.
- A menu item for the action choice list at the bottom of a list.
- A related link at the bottom of a list.

Note: To hide or restrict the New or Edit UI action on related list, use list control.
<table>
<thead>
<tr>
<th>Change Requests</th>
<th>Now</th>
<th>Go to Number</th>
<th>Search</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>Short Description</td>
<td>Approval</td>
<td>Type</td>
</tr>
<tr>
<td>CHG90000012</td>
<td>Java App Server</td>
<td>Normal</td>
<td>New</td>
</tr>
<tr>
<td>CHG90000011</td>
<td>Another Java App Server change</td>
<td>Normal</td>
<td>New</td>
</tr>
<tr>
<td>CHG90000010</td>
<td>Java Application change</td>
<td>Normal</td>
<td>New</td>
</tr>
<tr>
<td>CHG90000009</td>
<td>Apply patches 10.2.10.3</td>
<td>Normal</td>
<td>New</td>
</tr>
<tr>
<td>CHG90000008</td>
<td>Install new Cisco</td>
<td>Normal</td>
<td>New</td>
</tr>
<tr>
<td>CHG90000007</td>
<td>R &amp; D wants to know if it's worth to switch over to Linux desktops</td>
<td>Normal</td>
<td>New</td>
</tr>
<tr>
<td>CHG90000006</td>
<td>Put another 100 GB drive on the 2nd Floor Server</td>
<td>Normal</td>
<td>New</td>
</tr>
<tr>
<td>CHG90000005</td>
<td>Install new PIBX</td>
<td>Approved</td>
<td>Normal</td>
</tr>
<tr>
<td>CHG90000004</td>
<td>Upgrade to Oracle 11i</td>
<td>Normal</td>
<td>New</td>
</tr>
<tr>
<td>CHG90000003</td>
<td>Reinstall Oracle Virtual Server</td>
<td>Requested</td>
<td>Normal</td>
</tr>
<tr>
<td>CHG90000002</td>
<td>New</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **List banner button**
- **Right-click list context menu**
- **List choice**
- **List bottom button**
Create a UI action

You can create a new UI action or edit an existing one.

Role required: ui_action_admin or admin

You can add UI actions to tables and database views that are in the same scope as the UI action and tables that allow UI actions from another application scope to run on them.

1. Navigate to **System Definition > UI Actions**.
2. Click **New** or open an existing record.
3. Define the UI action by completing the fields.
   You may need to configure the form to see all the fields.

<table>
<thead>
<tr>
<th><strong>Field</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Defines the text that appears on the button, link, or context menu item.</td>
</tr>
<tr>
<td>Table</td>
<td>Defines the table on which the UI action is available. By default, the UI action also appears on tables that extend the selected table (for example, Task actions appear on the Incident table). Select <strong>Global</strong> to make the action available on all tables.</td>
</tr>
<tr>
<td>Order</td>
<td>Defines the order in which the UI action appears. The order applies to buttons from left to right and to menu actions from top to bottom.</td>
</tr>
<tr>
<td>Action name</td>
<td>Defines a name to use when referencing the UI action in scripts.</td>
</tr>
<tr>
<td>Active</td>
<td>Enables the UI action when selected. To disable a UI action, clear the check box.</td>
</tr>
<tr>
<td>Show insert</td>
<td>Shows a button on new records that have not been inserted.</td>
</tr>
<tr>
<td>Show update</td>
<td>Shows a button on existing records.</td>
</tr>
<tr>
<td>Client</td>
<td>The UI action executes its script in the user's browser, not on the server. When enabled, the <strong>OnClick</strong> field appears above the Condition field.</td>
</tr>
<tr>
<td>List v2 Compatible</td>
<td>Indicates that the UI action is compatible with v2 lists. This field must be enabled to display the UI action in a v2 list, but only if the <strong>List v3 Compatible</strong> field is enabled as well. If the <strong>List v3 Compatible</strong> field is not enabled, the UI action displays in v2 lists regardless of the <strong>List v2 Compatible</strong> field state.</td>
</tr>
<tr>
<td>List v3 Compatible</td>
<td>Indicates that the UI action is compatible with v3 lists. This field must be enabled to display the UI action in a v3 list.</td>
</tr>
<tr>
<td>Form button</td>
<td>Puts a button on a form.</td>
</tr>
<tr>
<td>Form context menu</td>
<td>Puts an item in a form context menu (right-click the form header).</td>
</tr>
<tr>
<td>Form link</td>
<td>Puts a link in the Related Links section of a form.</td>
</tr>
</tbody>
</table>
### Field | Description
---|---
List banner button | Puts a button in the banner of a list.
List bottom button | Puts a button at the bottom of a list.
List context menu | Puts an item in a list field context menu (right-click a cell in a list).
List choice | Puts an item in the action choice list at the bottom of a list.
List link | Puts a link in the Related Links section at the bottom of a list.
Overrides | Specifies a UI action that this UI action overrides.
Comments | Provides descriptive content regarding this UI action.
Hint | Defines the text that appears when a user points to the UI action control.
Onclick | The name of the JavaScript function to run when the UI action is executed. The function is defined in the **Script** field.
Condition | Defines the conditions that restrict when a UI action appears. See Using the condition builder to customize UI actions for Agent Workspace for examples.
Script | Defines the script to run when the UI action is executed.
Related lists on the form view:
UI Action Visibility | Specifies other views of the form that the UI action applies to. Use this option to restrict the UI action to form views that you specify.
Versions | Shows all versions of the UI action. Use this list to compare versions or to revert to a previous version.

4. Click **Submit** or **Update**.

**Note:** If the UI action is enabled to run on the client side, wrap it in a function. Otherwise, the contents of the **Script** field runs when the page loads.

As part of a UI action script, you can redirect a user to a URL. For example, you might add links to a form or open a new record after it is created from a UI action. To redirect a user to a URL from a UI action, use this syntax in the **Script** field to define the redirect link:

```javascript
action.setRedirectURL ('http://www.mysite.com/mypage.htm');
```

To direct a user to a record, use this syntax, where **new_record** is the variable name for the GlideRecord:

```javascript
action.setRedirectURL (new_record);
```
Using the condition builder to customize UI actions for Agent Workspace

Configure UI actions by adding conditions to a UI Action form.

Using the UI action condition builder

The following condition is configured for the Close Incident button:

For this action to appear on a form, these conditions must evaluate to true:

- `current.incident_state` must equal 6: The incident must already be in a Resolved state.
- `gs.hasRole("itil_admin")`: The current user must have the itil_admin role.

OR this condition must evaluate to true:

- `gs.getUserID() == current.caller_id`: The current user is the user who requested the change.
Note:

- The current object is not available for conditions on a list context menu. The list context menu option is selected. Any use of current on these actions is ignored.
- You can reference the parent record for the UI action conditions on a related list button. For example, to disable the New and Edit buttons on the Affected CIs related list for closed changes, copy the global m2m UI actions to the task_ci table and add a condition of parent.active.
- If you leave one of the fields empty that you specify in your condition statement, that condition defaults to true.

Restricting UI actions based on form views

You can restrict UI actions to appear only on specified form views.

Use the UI Action Visibility related list on the UI Action form to restrict a UI action by view. A UI action is available for the specified view according to the following rules:

1. If there are no visibility rules, the action appears on all views.
2. Any exclude rule on a given view means that the action does not appear on that view.
3. If there is at least one include rule, then the action appears only on views that are specifically included.

Example: Show an action everywhere except the Cost Management view

Add an exclude rule for the Cost management view.

Example exclusion UI action view
Example: Show an action on the Routine and ITIL views, but nowhere else

Add include rules for the Routine and ITIL views.

Override a UI action for an extended table

You can override or remove a UI action for a table that is extended from another table.

When a UI action is defined for the Task table, it applies to all tasks, including incidents, changes, problems, and any other tables that extend the Task table. Similarly, a global UI action applies to every table. However, you can override a UI action for a specific table. This example demonstrates how to override or remove a UI action on the Task [task] table for only the Incident [incident] table.

1. Complete the following steps to override a UI action on the Task table for just the Incident table.
   a) Create a UI action on the Incident table with the same Action name.
      If the Action name is not defined, update both the new UI action and the UI action to be overridden with the same Action name.
   b) Enter a script that is specific to the Incident table.

2. Complete the following steps to remove a UI action on the Task table for the Incident table.
   a) Navigate to the UI action definition for the Task table.
   b) Add the condition `current.getRecordClassName() != 'incident'`.
UI policies

UI policies dynamically change the behavior of information on a form and control custom process flows for tasks. For example, you can use UI policies to make the number field on a form read-only, make the short description field mandatory, and hide other fields. Basic UI policies do not require any scripting, however for more advanced actions, use the **Run scripts** option.

You can also use client scripts to perform all of these actions, but for faster load times use UI policies when possible.

Create a UI policy

Create a UI policy to define custom process flows for tasks.

Role required: **ui_policy_admin**

A UI policy condition evaluates all fields even if they are not visible on the form. This function removes the requirement that a field must be on a form for it to be evaluated.

**Note:**

- Policies carried over from versions prior to Fuji are evaluated differently. Fields that previously were not evaluated are evaluated.
- UI policies are not supported on search screens.
- UI Policies also apply to forms and lists displayed within Content Management System application.

1. Navigate to **System UI > UI Policies**.
2. Click **New**. The UI Policy [Advanced view] form opens
3. To change the view, in **Related Links** click **Default view**.
4. Complete the form, as appropriate.
   You may need to configure the form to see all the fields.

**UI policy fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>The table for the form to be modified.</td>
</tr>
<tr>
<td>Active</td>
<td>The active status of the UI policy. Only active UI policies are applied.</td>
</tr>
<tr>
<td>Short description</td>
<td>Short summary of the UI policy.</td>
</tr>
<tr>
<td>Order [Advanced view]</td>
<td>The processing sequence, from the lowest to highest number. If two policies conflict, the UI policy with the higher number executes. For inherited UI policies, the extended (child) table's UI policies are executed first. Then the base table UI policies are executed; both from lowest to highest specified value.</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conditions</td>
<td>The conditions which, if fulfilled, cause the UI policy to be applied. Conditions are built with the condition builder. To set conditions using a script, use a client script instead. Conditions are only rechecked if a user manually changes a field on a form. If the change is made by a UI action, context menu action, or through the list editor, it is not evaluated.</td>
</tr>
<tr>
<td>Global [Advanced view]</td>
<td>Option for specifying whether the UI policy applies to all form views. If this check box is cleared, the UI policy is view-specific. By default, the Global UI policy applies to all form views. However, a UI policy can be specific to a view. For example, you can define a UI policy for only the itil view of a form. Use the View field to accomplish this.</td>
</tr>
<tr>
<td>View [Advanced view]</td>
<td>Option for indicating which form view the UI policy applies to. This field is visible only if Global is not selected. If Global is not selected and the View field is left blank, the script applies the default view. For more information on form views, see View management.</td>
</tr>
<tr>
<td>Reverse if false [Advanced view]</td>
<td>Option for specifying that the UI policy action should be reversed when the conditions of its UI policy evaluate to false. In other words, when the conditions are true, actions are taken and when they change back to false, the actions are reversed (undone).</td>
</tr>
</tbody>
</table>
| On load [Advanced view]       | Option for specifying that the UI policy behavior should be performed OnLoad as well as when the form changes. You can check or clear the On load check box in a UI policy to control whether it runs every time a form is loaded when the conditions are satisfied. In this example, an administrator does not want an incident to enter the Awaiting user info state unless the user provides an explanation to the customer. The administrator creates a UI policy with the following settings.  
• In the When to Apply section, adds the condition [State] [is] [Awaiting user info] and clears the On load check box. This condition means that the UI policy applies only when the state is changed to Awaiting user info.  
• In the UI Policy Actions related list, creates a record that makes the Additional comments field mandatory when the condition is met. |
### Field

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Inherit [Advanced view]                    | Option for specifying whether extended tables inherit this UI policy. When a child table has an inherited UI policy from its parent table, the UI policy on the child table always runs first. This event is true regardless of the **Order** of the UI policies. Consider the following example:  
  • A child table has a UI policy with **Order** value 500 that shows the Urgency field when its conditions are met.  
  • Its parent table has a UI policy with the same conditions that hides the Urgency field. The parent table UI policy has **Order** value 100.  
  • Although the parent table **Order** field has a lower value, the child UI policy runs first and then the parent UI policy runs. When the conditions are met, the Urgency field is hidden. |

### Script

<table>
<thead>
<tr>
<th>Run scripts [Advanced view]</th>
<th>Option for specifying whether advanced behavior can be scripted for both true and false conditions.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execute if true [Advanced view]</td>
<td>A script that executes when the conditions of the UI policy are fulfilled. This field is available only if Run scripts is selected.</td>
</tr>
<tr>
<td>Execute if false [Advanced view]</td>
<td>A script that executes if the conditions of the UI policy are not fulfilled and the Reverse if false option is selected. This field is available only if Run scripts is selected.</td>
</tr>
</tbody>
</table>

### Other fields

<table>
<thead>
<tr>
<th>Run scripts in UI type</th>
<th>The UI type for this UI policy: Desktop, Mobile / Service Portal, or Both.</th>
</tr>
</thead>
</table>

### Related List: UI Policy Actions

<table>
<thead>
<tr>
<th>Table</th>
<th>[read-only] Field the UI policy action applies to.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field name</td>
<td>Field on the selected table to which the UI policy performs an action if true.</td>
</tr>
</tbody>
</table>

**Note:** If the specified field is not found on the form, the UI policy performs the action on the variable with the same name.

<table>
<thead>
<tr>
<th>Mandatory</th>
<th>Choice list for specifying how the UI policy affects the mandatory state of the field. Choices are:</th>
</tr>
</thead>
</table>
|           | • Leave alone  
|           | • True  
<p>|           | • False |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Visible            | Choice list for specifying how the UI policy affects the visible state of the field. Choices are:  
|                    | • Leave alone                                                               |
|                    | • True                                                                      |
|                    | • False                                                                     |
| Read only          | Choice list for specifying how the UI policy affects the read-only state of the field. Choices are:  
|                    | • Leave alone                                                               |
|                    | • True                                                                      |
|                    | • False                                                                     |

### Related Links

| Default view or Advanced view | Changes the form view to the default or advanced view. The fields change based on the view. |

5. Click **Submit**.

**Example: creating a UI policy**

Create a UI policy to implement controls in the Incident form when the state changes to **Resolved**.

Role required: **ui_policy_admin**

This example demonstrates how to implement the following controls.

- Make a **Close Notes** field mandatory.
- Hide the **Opened by** field.
- Make the **Priority**, **Severity**, and **Urgency** fields read-only.
- Run a client script that displays an alert message.

1. Navigate to **System UI > UI Policies**.
2. Click **New**.
3. Supply the following information.

**New UI policy**

<table>
<thead>
<tr>
<th>Name</th>
<th>Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>Incident</td>
</tr>
<tr>
<td>Conditions</td>
<td>[Incident state] [is] [Resolved]</td>
</tr>
<tr>
<td>Reverse if false</td>
<td>Select this check box. If the incident state is not <strong>Resolved</strong>, the UI policy is reversed.</td>
</tr>
<tr>
<td>On load</td>
<td>Select this check box to perform the actions when the form is loaded or when the condition changes.</td>
</tr>
</tbody>
</table>

4. Right-click the form header and select **Save** from the context menu.

The **UI Policy Actions** related list appears.

5. In the related list, click **New**.
6. Provide the following information.

**New UI policy actions**

<table>
<thead>
<tr>
<th>Name</th>
<th>Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field name</td>
<td>Close notes. This UI action makes the Close notes field mandatory.</td>
</tr>
<tr>
<td>Mandatory</td>
<td>True</td>
</tr>
<tr>
<td>Visible</td>
<td>Leave alone</td>
</tr>
<tr>
<td>Read Only</td>
<td>Leave alone</td>
</tr>
</tbody>
</table>

7. Click **Submit**.

8. Repeat the process to create UI policy actions to hide the **Opened by** field, and to make the **Priority**, **Severity**, and **Urgency** fields read-only.

**Client scripts for UI policies**

Any scripts you create for UI policies run on the client side.

You can use different options in the UI Policy form to control when and how the UI policy is applied. These options include client scripts, OnLoad execution, and view-specific UI policies. Administrators can use the UI Policy form to create client scripts that run `onChange` when the UI policy conditions are met (`Execute if true`) or not met (`Execute if false`). To display these scripting fields in the UI Policy form, in the Script section, select the **Run scripts** check box.

For example, to display an alert to the user when the incident **State** field changes to **Resolved**, create the following script in the **Execute if true** field.

```javascript
function onCondition(){
  alert('You changed the "Incident state" to Resolved. Please enter your comments in the "Close notes" field.');
}
```

**Advanced form configuration**

Administrators can configure advanced form features, such as form focus, form splits, and derived fields.

**Allow insert options on task records**

The **Insert** and **Insert and Stay** options are disabled by default for task records such as incidents and change requests. You can set a system property to show these options for task records.

Role required: admin

1. Navigate to **System Properties > UI Properties**.
2. Locate the property **Allow the use of the "Insert" and "Insert and Stay" options on task derived tables**. (`glide.ui.task.insert`)
3. Select the check box to enable or clear the check box to disable (default) the options for tasks.
4. Click **Save**.
Disable first field form focus

By default, forms set focus on the first writable field on the form. An administrator can disable form focus with a system property to make the form more accessible to users who use screenreaders.

Role required: admin

1. Navigate to *System Properties > UI Properties.*
2. Set the property `glide.ui.focus_first_element` to `false`.

With first field focus disabled, the form focuses on the first element on the page instead. Focusing on the first element, instead of the first writable element, helps orient users who use screenreaders so they can find all the elements on a form.

Disable the template bar

Administrators can disable the template bar on a table by creating a system property.

Role required: admin

Creating a table-specific property and setting it to false prevents users from displaying the template bar on a record for the specified table.

1. Navigate to *sys_properties.list.*
2. with the following settings.

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td><code>glide.ui.show_template_bar.&lt;TABLENAME&gt;</code></td>
</tr>
<tr>
<td>Type</td>
<td>`true</td>
</tr>
<tr>
<td>Value</td>
<td><code>false</code></td>
</tr>
</tbody>
</table>

3. Click *Submit.*

Modify form focus with a client script

By default, forms set focus on the first writable field on the form. An administrator can change that functionality to focus on other fields in the form for UI15 and earlier versions of the UI.

Modify the form focus with `onLoad()` client script on the form.

**Note:** The method `g_form.getElement` has been deprecated in UI16.

```javascript
function onLoad () {
  setTimeout ( function() {
    var refocus = g_form.getElement('table_name.field_name');
    refocus.focus();
  }, 0 );
}
```

Based on the nature of the field you are targeting, replace `table_name.field_name` with the appropriate value:

- For non-reference fields, enter the name of the field to focus on (for example, `short_description`).
- For reference fields, use the format `sys_display.table_name.field_name` (for example, `sys_display.incident.caller_id`).

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Deactivate form submission with the Enter key

By default, when you press the Enter key in a simple one-line text field, a choice list, or a Boolean field, the form is submitted.

Role required: admin

You can use a system preference to deactivate this feature if you do not want the Enter key to submit the form.

1. From the left navigation pane, select User Administration > User Preferences.
2. Select the enter_submits_form preference.
3. Set the value to false.
4. Click Update.
   
   The change does not take effect until user preferences are reloaded either at login or when a session is created.

Enable multiple form splits

Form splits enable you to organize fields on a form into columns. Administrators must add a property to enable form splits.

Role required: admin
Configuration of two form splits

<table>
<thead>
<tr>
<th>Asset tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
</tr>
<tr>
<td>Serial number</td>
</tr>
<tr>
<td>Substate</td>
</tr>
</tbody>
</table>

| Assigned to |
| Stockroom |
| Reserved for |
| Managed by |
| Owned by |
| Parent |
| Class |

| Location |
| Department |
| Company |

| Assigned |
| Installed |

| Comments |

---
Example of the form with two form splits

When you organize fields in this manner and the user is viewing the form on a small mobile device, the fields within the first split are listed before the fields in the second split. In this example, the Asset tag, State, Serial number, and Substate field are listed before any of the fields below them. You can also create elements that span the form at the top of the form.

1. Enter sys_properties.list in the Navigation filter.
   The entire list of properties in the System Properties [sys_properties] table appears.
2. If the property does not exist, click New.
3. Enter the following information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>glide.ui.form_multiple_splits</td>
</tr>
<tr>
<td>Description</td>
<td>Enable multiple form splits</td>
</tr>
<tr>
<td>Type</td>
<td>true</td>
</tr>
<tr>
<td>Value</td>
<td>true</td>
</tr>
</tbody>
</table>

4. Click the form context menu icon and select Save.
   The Categories related list appears.
5. Click Edit and move UI to the Categories List.
6. Click Save.
   The System Property form reopens and the new property appears in the UI Properties page.
Define required fields

You can specify which form fields are required in forms. This action prevents users with the personalize_form role from removing the field by configuring the form layout.

Role required: admin

The Required Form Fields plugin must be active.

If present on a form, only an administrator can remove required fields. When you configure a form, required fields appear in a gray color and have a tooltip indicating they are required. Required fields are defined in the Required Form Fields [sys_ui_element_required] table.

The expected (although not the only) use case for this feature is as part of a delegated administration scheme. For example, you can grant branch offices the rights to modify forms by granting the personalize_form role, but not allow them to remove certain fields which are critical to overall business processing.

1. Navigate to sys_properties.list.
2. Locate the property named glide.ui.form.enforce_required_fields and make sure it is set to true.
3. Navigate to System UI > Required Form Fields.
4. Click New.
5. Select the table and field, and then select the Required check box.
   The following example sets the Short description field on the Incident form to be required.

   ![Required Form Field Configuration]

   If you decide later that you do not want to make the field required, clear the Required checkbox. This action is preferable to deleting the record.

6. Click Submit.

If the table specified has extension tables, then the Required Form Field record applies to forms of all extended tables. For example, if an administrator specifies that the Short description field is required for the Task table, then this configuration applies to the Incident form, Change Request form, Problem form, and so on.

An extended table can override the Required Form Field rule of its base table. For example, if the Short description field is required for the Task table, but not required for the Incident table, it is required for all Task tables except Incident.
Control the label type for derived fields

You can configure the type of label that appears for derived fields.

Role required: admin

An example would be displaying the email address for the caller when looking at an incident record. The email address is not stored in the Incident table, but is obtained by following the caller reference from the incident to the User table. You control the label type by setting a system property. For example, the field label for an incident email address can be either of the following strings.

- **Caller Email**, which represents the complete label to uniquely identify this field as the email from the caller user record. If you display the email address for the person the ticket is assigned to, its label would be **Assigned to Email**.
- **Email** which is the label for the target field. This label is not unique on the form if, for example, you are also displaying the email address of the person assigned to the incident. However, usually the placement of the field on the form makes it clear what the field represents.

1. Navigate to **System Properties > System**.
2. Locate the **Use short labels for all fields.** For example, if a form contains the caller’s email address, use the "Email" label rather than the full label of "Caller Email" (glide.short.labels) property.

   The default value is **true**, meaning that the short label is displayed in all forms.

3. If you want to display the complete label in forms, clear the check box.

4. Click **Save**.

---

**Field administration**

The individual pieces of data in a record are called fields. Users enter data in fields on the form or by using the list editor. Administrators can create new or modify existing fields.

Users can enter data in fields by using the list editor or by using a form. In form view, fields appear as fields in the form, and in list view they appear as columns of data in the table. Administrators can create new fields or change the type of existing fields.

**Field types**

These field types are available to administrators when creating new fields or changing the type of existing fields.

<table>
<thead>
<tr>
<th>Field Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio</td>
<td>Field for uploading and embedding .mp3 or .ogg audio files.</td>
</tr>
<tr>
<td>Choice</td>
<td>List of configurable choices.</td>
</tr>
<tr>
<td>Collection</td>
<td>Dictionary entries with the Collection type represent the table rather than a field on the table. Changes such as attributes or the Read only check box applied to this entry are applied to the table rather than a specific field. This entry is automatically created when a table is created. There should not be more than one entry for a table of this type.</td>
</tr>
<tr>
<td>Color</td>
<td>String field that accepts CSS color declarations (including hex or RGB notation) and displays a preview. To learn more, see <a href="https://developer.mozilla.org/en-US/docs/Web/CSS/color_value">https://developer.mozilla.org/en-US/docs/Web/CSS/color_value</a>.</td>
</tr>
<tr>
<td>Condition String</td>
<td>Text field that accepts a plain JavaScript condition statement that is validated automatically for correctness before an update.</td>
</tr>
<tr>
<td>Conditions</td>
<td>Field that adds the condition builder to a form. You must specify a dependent field that references the table name.</td>
</tr>
</tbody>
</table>

**Note:** If you edit a field on a child table that is present on the parent table, it is also changed in the parent table and all other child tables.

**Note:** If a table column identifier is created using Kanji characters, it is ignored in any update or insert operation from a form. Kanji characters are not currently supported.
<table>
<thead>
<tr>
<th>Field Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Currency</td>
<td>Decimal field with four digits after the decimal point. When displayed on a form, a currency field also includes an additional choice list for selecting the currency type. If there is no default value for the field, empty currency fields use the reference currency. Adding a value causes the field to use the session currency of the active user. See Change default currency decimal places for how to use two fraction digits.</td>
</tr>
<tr>
<td>Note: Once you assign this type to a field, you cannot change it to an FX Currency type.</td>
<td></td>
</tr>
<tr>
<td>Data Structure</td>
<td>Field that allows the selection of one of the following data structures and entry of values to organize particular information in the record.</td>
</tr>
<tr>
<td></td>
<td>- String</td>
</tr>
<tr>
<td></td>
<td>- Boolean</td>
</tr>
<tr>
<td></td>
<td>- Integer</td>
</tr>
<tr>
<td></td>
<td>- Decimal</td>
</tr>
<tr>
<td></td>
<td>- Object</td>
</tr>
<tr>
<td></td>
<td>- Array</td>
</tr>
<tr>
<td>Date</td>
<td>Day, which can be selected with a calendar widget.</td>
</tr>
<tr>
<td>Date/Time</td>
<td>Day and time of day, which can be selected with a calendar widget.</td>
</tr>
<tr>
<td>Decimal</td>
<td>Number with up to two digits after the decimal points (for example, 12.34).</td>
</tr>
<tr>
<td>Document ID</td>
<td>Reference to any record on any table.</td>
</tr>
<tr>
<td>Domain ID</td>
<td>System field that contains a reference to the domain.</td>
</tr>
<tr>
<td>Due Date</td>
<td>String input field that stores a date-time.</td>
</tr>
<tr>
<td>Duration</td>
<td>Length of time. Stored in the database as an integer number of milliseconds, but appears in days, hours, minutes, and seconds.</td>
</tr>
<tr>
<td>Encrypted Text</td>
<td>Field that is encrypted for security. Depending on the user's encryption context, the field may be hidden, the value may be hidden, or the field and value may display.</td>
</tr>
<tr>
<td>Field Name</td>
<td>Reference field for a field name in the table selected in a Table Name field type. Make this field dependent on the Table Name field.</td>
</tr>
<tr>
<td>File Attachment</td>
<td>Field for holding a file. A field holds one file. All file types are supported.</td>
</tr>
<tr>
<td>Floating Point Number</td>
<td>Number with up to seven digits after the decimal point.</td>
</tr>
<tr>
<td>Field Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>FX Currency</td>
<td>Also known in internal code as Currency2 fields, this field type is an alternative to the standard (default) currency fields found in most Now Platform® applications. This type of currency field is highly configurable, supports custom rate tables, report aggregations, and provides for improved visibility into conversion calculations. To learn more about the FX Currency field type, see Setting up and using FX Currency fields.</td>
</tr>
<tr>
<td>Note:</td>
<td>Once you assign this type to a field, you cannot change it to an Currency type.</td>
</tr>
<tr>
<td>HTML</td>
<td>String field with a built-in HTML editor.</td>
</tr>
<tr>
<td>Icon</td>
<td>String field that provides the user access to an icon picker in a form. By default, the favorites icon set is used.</td>
</tr>
<tr>
<td>Image</td>
<td>Field for uploading and embedding images.</td>
</tr>
<tr>
<td>Integer</td>
<td>Number with zero decimal points.</td>
</tr>
<tr>
<td>IP address</td>
<td>Variable character field that stores IPv4 and IPv6 addresses. See IP address field type for more information.</td>
</tr>
<tr>
<td>Journal</td>
<td>Field that accepts text entries and displays previous entries with a user name and time stamp.</td>
</tr>
<tr>
<td>Journal Input</td>
<td>Field that accepts text entries but does not display previous entries.</td>
</tr>
<tr>
<td>Journal List</td>
<td>Field that displays the contents of journal fields. You must specify the journal fields as the dependent fields. If a journal list field depends on more than one journal field, the entries are displayed chronologically.</td>
</tr>
<tr>
<td>List</td>
<td>Reference field that accepts multiple references rather than just one.</td>
</tr>
<tr>
<td>Long</td>
<td>Integer field that can contain a longer number than the integer field.</td>
</tr>
<tr>
<td>Field Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Name-Value Pairs</td>
<td>Field that maps text values. Each mapping is one-to-one, however a single Name-Value Pairs field can contain multiple mappings. Each mapping must use a unique name, and the name cannot be empty. For example, you can use a Name-Value Pairs field to hold header information for a web service request. In this example, the name of each mapping is the header such as Content-Type and the value is the header value, such as Application/json. For information on scripting Name-Value Pairs fields, see Name-value pairs field type.</td>
</tr>
<tr>
<td>Password (1 Way Encrypted)</td>
<td>Text field that stores passwords with one-way encryption. One-way encryption stores the password as a secure hash value that cannot be decrypted.</td>
</tr>
<tr>
<td>Password (2 Way Encrypted)</td>
<td>Text field that stores passwords with two-way encryption. Two-way encryption stores the password as a secure encrypted value that can be decrypted programmatically within the instance. You can use Password 2 encryption with form variables. To encrypt text fields on forms, use Encryption Contexts. The length for password2 field values must be at least 255 characters.</td>
</tr>
<tr>
<td>Percent Complete</td>
<td>Decimal field that renders a percent complete bar in lists. You can convert any existing decimal field to a percent complete field.</td>
</tr>
<tr>
<td>Phone Number (E164)</td>
<td>String field that provides E164-compliant formatting and validation for telephone numbers.</td>
</tr>
<tr>
<td>Price</td>
<td>A currency field that enables control over conversions and display. See Price fields for more information.</td>
</tr>
<tr>
<td>Reference</td>
<td>Query that displays records from another table.</td>
</tr>
<tr>
<td>Script</td>
<td>Text field that accepts JavaScript code input and provides controls, such as syntax checking and formatting. It also provides a list of fields and server APIs. You must specify a dependent field that references the table name for the list of fields.</td>
</tr>
<tr>
<td>Script (Plain)</td>
<td>Text field that accepts JavaScript code input and provides controls, such as syntax checking and formatting.</td>
</tr>
<tr>
<td>Field Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>String</td>
<td>For 255 characters or less, the string field is a single-line text field. Anything 256 characters or over appears as a multi-line text box. Note: The database may translate the value that you provide in the Max length field to the closest matching database field type. For example, a max string length of 80 maps to the nearest database field type of VARCHAR(100). For Oracle instances, users are not able to increase the max length of a string field to a value greater than 4000 through the application UI. Changes greater than 4000 require the CLOB data type in Oracle. If you require a field to be larger than 4000 characters, log an incident to request the change.</td>
</tr>
<tr>
<td>String (Full UTF-8)</td>
<td>A string field that can contain UTF-8 character encoding. This field has the same restriction as the String data type as to maximum length that a user can define within the application UI. Emoji Support: The String (Full UTF-8) field type does, and should be used if we expect to use emojis in a field. There is slightly more overhead when using the Full UTF-8 type.</td>
</tr>
<tr>
<td>Suggestion</td>
<td>String field that provides suggested values but accepts free-form text. Available when you add a field by configuring a form or list. Otherwise, you must modify the dictionary entry of an existing string or journal field.</td>
</tr>
<tr>
<td>Table Name</td>
<td>String field that lets you select a table. If you use the Field Name field type, add this field type and make the Field Name field dependent on the Table Name field.</td>
</tr>
<tr>
<td>Time</td>
<td>Specific time. Stored in the database as a date/time field. Only the time part of this field is used. Note: This field always stores the date as 1970-01-01, which does not fall within the dates for Daylight Savings Time (DST). As a result, the time is not automatically adjusted for DST. If a custom feature uses time as a start time, it is the responsibility of the feature to adjust for DST, if necessary.</td>
</tr>
<tr>
<td>Translated HTML</td>
<td>HTML field that displays different translations that are based on the user's language.</td>
</tr>
<tr>
<td>Translated Text</td>
<td>Text field that displays different translations that are based on the user's language.</td>
</tr>
<tr>
<td>True/False</td>
<td>Boolean field that appears as a one-digit integer, typically 1 (true) or 0 (false).</td>
</tr>
</tbody>
</table>
### Field Type | Description
--- | ---
URL | String field that is a clickable URL field when locked. **Note:** In the mobile UI, this field appears as a multi-line text field. The field saves as a single line, with the line breaks removed.
Video | Field for uploading and embedding video.
Wiki | String field with a built-in Wiki text editor that accepts a simplified version of standard Wiki text formatting.
Workflow | Choice list field that displays a stage in a workflow.

**Note:** When you create a custom field, use one of these supported field types. Other field types, such as User Input, are for internal use only and are not supported for custom fields.

### Choice list field type

A choice list is a type of field that lets the user select from a pre-defined set of choices.

Administrators can define the available choices and customize the behavior and appearance of choice lists.

#### Incident state choice list

**Note:** Choice lists do not support a one to many relationship. Only one choice from a choice list can be selected at a time.

### Choice list security

You can use the personalize_choices security role to enable non-administrators modify Choice elements options on all tables.

If more granular control is desired, you can also create a custom ACL (security rule) governing the personalize_choices operation either for a particular field or for all fields (*) on a particular table. However, access to the personalize_choices operation on a particular field does not confer the ability to add new choices for that field.

To be able to create new choices for a particular field, an ACL that grants personalize_choices access for that field is required. For example, to give the hris_admin role the ability to personalize only the Category field for Human Resources KB articles, you need an ACL granting personalize_choices access to the hris_admin role on the Category field of the Knowledge (kb_knowledge) table.
There are predefined ACLs granting both types of access to the personalize_choices security role, for all fields on all tables. The personalize_choices security role also has read, write, and delete access to the sys_choices table. However, this additional access is not required when making just the Personalize Choices functionality available on a granular basis.

To be able to create new choices for a particular field, an ACL that grants personalize_choices access for that field is required. For example, to give the hris_admin role the ability to personalize only the Category field for Human Resources KB articles, you need an ACL granting personalize_choices access to the hris_admin role on the Category field of the Knowledge (kb_knowledge) table.

**Values to associate with choice labels for scripting**

When you write a script that references a choice list, you need to know the value that is associated with each choice.

For example, to check whether the incident_state field is active, you could not use the condition `current.incident_state == "active"` because the value associated with the choice labeled **Active** is the integer 2. Instead, you would use the condition `current.incident_state == 2`.

The **Type** field on the choice list dictionary entry determines the data type of the values.

To determine the value associated with a choice, right-click the field label and select **Show Choice List**, and then locate the choice for which you need to know the value.

<table>
<thead>
<tr>
<th>Table</th>
<th>Element</th>
<th>Language</th>
<th>Value</th>
<th>Label</th>
<th>Inactive</th>
<th>Sequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>incident</td>
<td>state</td>
<td>en</td>
<td>1</td>
<td>New</td>
<td>false</td>
<td>1</td>
</tr>
<tr>
<td>incident</td>
<td>state</td>
<td>en</td>
<td>2</td>
<td>Active</td>
<td>false</td>
<td>2</td>
</tr>
<tr>
<td>incident</td>
<td>state</td>
<td>en</td>
<td>3</td>
<td>Awaiting Problem</td>
<td>false</td>
<td>3</td>
</tr>
<tr>
<td>incident</td>
<td>state</td>
<td>en</td>
<td>4</td>
<td>Awaiting User Info</td>
<td>false</td>
<td>4</td>
</tr>
<tr>
<td>incident</td>
<td>state</td>
<td>en</td>
<td>5</td>
<td>Awaiting Evidence</td>
<td>false</td>
<td>5</td>
</tr>
<tr>
<td>incident</td>
<td>state</td>
<td>en</td>
<td>6</td>
<td>Resolved</td>
<td>false</td>
<td>6</td>
</tr>
<tr>
<td>incident</td>
<td>state</td>
<td>en</td>
<td>7</td>
<td>Closed</td>
<td>false</td>
<td>7</td>
</tr>
</tbody>
</table>

**Show choices list values**

The **-- None --** option may not have a sys_choice record associated with it. A choice list field set to **-- None --** evaluates to these values, depending on the script context as listed below.

- For client-side scripts, such as client scripts: "" (empty string)
- For server-side scripts, such as business rules: "0" (string of the number zero)

**Integer values for default choice lists**

Choice provide four default values.

Some common choice lists use integer values that do not match the string labels. For example, the Problem table uses these default values for the **State** field.
State field default values

<table>
<thead>
<tr>
<th>Value</th>
<th>Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Open</td>
</tr>
<tr>
<td>2</td>
<td>Known Error</td>
</tr>
<tr>
<td>3</td>
<td>Pending Change</td>
</tr>
<tr>
<td>4</td>
<td>Closed/Resolved</td>
</tr>
</tbody>
</table>

These integer values are also used in several default business rules. For example, a business rule on the Incident table sets the active flag to false when the State field changes to 7, which is the default value for the Closed. If you change the values of your Incident state options, this business rule may no longer behave as desired or expected.

On the Incident table, the Active, State, and Incident state fields are affected by the following default business rules.

Default business rules

<table>
<thead>
<tr>
<th>Business rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mark_closed (incident)</td>
<td>If the incident_state changes to 7 (Closed), the Active field is set to false</td>
</tr>
<tr>
<td>incident reopen (incident)</td>
<td>If the incident_state is less than 7 (Closed) and the Active field is false, the Active field is set to true</td>
</tr>
<tr>
<td>mark closed (task)</td>
<td>If the state changes to either 3 (Closed Complete) or 4 (Closed Incomplete), the Active field is set to false</td>
</tr>
<tr>
<td>task closer (task)</td>
<td>If the Active flag changes from true to false and the state is neither 3 (Closed Complete) nor 4 (Closed Incomplete), the state is set to 3 (Closed Complete)</td>
</tr>
<tr>
<td>task reopener (task)</td>
<td>If the Active field changes from false to true and the state is either 3 (Closed Complete) or 4 (Closed Incomplete), the state is set to 1 (Open)</td>
</tr>
</tbody>
</table>

Note: Notice that these business rules do not change incident_state based on a change to either the Active field or the State field. Changes to incident_state drive the other two fields, not the other way around.

Configure state field choice values

State fields are a subset of choice list fields. Keep the following information in mind when you configure choice values for the state field.

- Use a negative value to add a new active state field.
- Search for and study the business rules that use a state number filter on the Script and Conditions fields. You can use the Debug tool to trace the order of the business rule execution.
- New values representing inactive states should have a value above 8.

You can define any of the following attributes for a state field by configuring the dictionary. If the attributes are not defined, the system uses the default values. The TaskStateUtil API uses the following attributes. For more information on the TaskStateUtil API, see TaskStateUtil.
Related Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>close_states</td>
<td>Semicolon delimited list of state values that are inactive, used to identify whether the task should be set to active or inactive. This is a required attribute to use the TaskStateUtil functionality.</td>
</tr>
<tr>
<td>default_close_state</td>
<td>Optional attribute to define the state value of the default close state if you want to define business rules that automatically close a task. Defaults to 3, typically Closed Complete if attribute is not defined.</td>
</tr>
<tr>
<td>default_work_state</td>
<td>Optional attribute to define the state value of the default working state if you want to define business rules that automatically set a task for working. Defaults to 2, typically Work in Progress if the attribute is not defined.</td>
</tr>
</tbody>
</table>

State modification examples

Follow these examples for modifying the states of incidents and change requests.

Role required: admin

1. Navigate to System Definition > Choice Lists.
2. At the top of the list, construct a list filter like the following:
   - Table: incident
   - Element: incident_state
3. Run the filter.
   Notice that the Closed state has a value of 7 and the Resolved state has a value of 6. Any state greater than or equal to 7 is assumed to be inactive. Therefore, you should use a positive integer greater than 7 if you want to add a new inactive-type of state. Use a negative value like -1 or -2 if you wish to add a new active-type of state field, such as Awaiting Vendor.
5. At the top of the list, construct a list filter like the following:
   - Table: change_request
   - Element: phase_state
6. Run the filter.
   Notice that the Complete state has a value of 8. Any state greater than or equal to 8 is assumed to be inactive. Therefore, you should use a positive integer greater than 8 if you want to add a new inactive-type of state, such as Cancelled. Use a negative value like -1 or -2 if you wish to add a new active-type of state field, such as Pending.

Troubleshoot change states and business rules

Business rules in the system make assumptions about state values. You can troubleshoot business rules to see the order in which they run and see how it affects changes you make to State field values.

Role required: admin

1. Navigate to System Definition > Business Rules.
2. Construct a filter like this one to view the scripts and conditions that pertain to the Resolved incident_state of 6 or the Closed incident_state value of 7:

   The **Script** field contains 7 OR the **Condition** field contains 7 OR the **Script** field contains 6 OR the **Condition** field contains 6 AND the **Table** field is incident AND the **Active** field is true.

See Debug Business Rule for information on how to trace the order of business rule execution. You can click **Debug All**, resolve an incident, and then check the trace at the bottom of form to watch the business rules execute. These two line examples show that the mark_closed business rule code is entered ==> and then exited <==

```plaintext
==> 'mark_closed' on incident
<= 'mark_closed' on incident
```

### View choice list definitions

The Choice Set [sys_choice_set] table contains a record for every field that uses a choice list.

Role required: personalize_choices

**Note:** The personalize_choices role must be explicitly granted to the user; it cannot be an ACL.

The choice set record is associated with an application file, which allows update sets and team development to track and transfer all choices for a field in a single update record.

Choice list values allow a maximum length of 40 characters. The range of allowable numerical values is [-999, 999].

1. Right-click the choice list field label and select **Show Choice List**.

   To view other choice list values, modify the filter at the top of the list.

   **Note:** When you use an ACL to grant personalize_choices on a particular field, **Show Choice List** is not available. It is only available if you explicitly grant the role to the user. **Configure Choices** continues to appear regardless of whether it is an ACL or an explicitly granted user role.

2. Review the items in the list.

   **Warning:** Do not add new choices to the list. To add new choices to a choice list field, use the **Configure Choices** option.

### Define an option for a choice list

You can personalize the options that are available in a choice list.

Role required: personalize_choices

1. Navigate to a form where the field appears.
2. If the choice list is dependent on another field, enter the choice value that the options depend on.

   For example, on the incident table, the **Subcategory** is dependent on the **Category**. To customize which subcategory choices are available for the hardware category, select **Hardware** in the **Category** field.

3. Right-click the field label and select **Configure Choices**.
4. Use the slushbucket to rearrange the order, add, or remove items or to create new items.
5. Click **Save**.

To dynamically add items to a choice list, use the `addOption` GlideForm method.

**Note:** Some business rules may be affected by changes to choice list options (for example, default Incident states).

---

**Reuse a choice list**

After defining a set of choice list values, you can reuse the values for another field in a different table.

Role required: personalize_choices

1. Right-click an existing choice field (Field A) and select **Configure Choices**.
2. Add the desired choice list values in the **Choices** related list.
3. To reuse the choice list values for another field (Field B) in a different table, right-click the label for Field B and select **Configure Dictionary**.
4. In the **Choice table** field, select the table where Field A resides.
5. In the **Choice field** field, select Field A.

---

6. Click **Update**.

The choice list values defined on Field A are displayed on Field B. When you add or remove choice list values on Field A, those changes are also reflected on Field B. After you specify a choice table and a choice field, the field no longer uses the defined choice list.

---

**Remove the None option from a choice list**

You can remove the **None** option from a choice list if it is not necessary.

Role required: personalize_dictionary

1. Navigate to a form where the field appears.
2. Right-click the field label and select **Configure Dictionary**.
3. Change the **Choice** field value to **Dropdown without -- None -- (must specify a default value)**.

![Choice field options](image)

4. Ensure that the **Default** field is populated to determine which choice is displayed by default.

   **Note:** If the field is dependent on another field, the **-- None --** option remains available.

**Change the None display value for a choice list**

You can change the default display label of the **None** option for a choice field.

Role required: personalize_choices

**Note:** The personalize_choices role must be explicitly granted to the user; it cannot be an ACL.

1. Navigate to a form on which the field appears.
2. Right-click the field label and select **Show Choice List**.
3. Click **New**.
4. Complete the form.

**Choice form fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>Select the table.</td>
</tr>
<tr>
<td>Element</td>
<td>Leave the name of the field that is automatically populated.</td>
</tr>
<tr>
<td>Language</td>
<td>Enter ISO language code for the label.</td>
</tr>
<tr>
<td>Sequence</td>
<td>Leave empty. This field determines the order.</td>
</tr>
<tr>
<td>Inactive</td>
<td>Leave cleared.</td>
</tr>
<tr>
<td>Field</td>
<td>Value</td>
</tr>
<tr>
<td>---------</td>
<td>-------</td>
</tr>
<tr>
<td><strong>Label</strong></td>
<td>Enter the label to appear in the choice list. You can use JavaScript, including calls to script includes, to define the label. For example, the JavaScript label in the following example changes the <strong>-- None --</strong> value of the <strong>Time zone</strong> choice list in a user record to use the time zone value of the instance.</td>
</tr>
<tr>
<td><strong>Value</strong></td>
<td>Enter <strong>NULL_OVERRIDE</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You must enter <strong>NULL_OVERRIDE</strong> as the value, or the new label appears in addition to the <strong>-- None --</strong> option.</td>
</tr>
<tr>
<td><strong>Dependent value</strong></td>
<td>Leave blank.</td>
</tr>
<tr>
<td><strong>Hint</strong></td>
<td>Leave blank.</td>
</tr>
</tbody>
</table>

5. Click **Submit**.

**Delete all choice list options**
You can delete all choices for a choice field from the Choice Set record.

Role required: personalize

You may want to use this method when you are developing a new application and the business requirements change. If you are updating a choice list that is already in use, consider deactivating the options you no longer use to avoid conflicts with existing data or scripts that may rely on the previous options.

1. In the navigation filter, enter `sys_choice_set.list` and press Enter.
2. Open the choice set record for the field.
   For example, to locate the choice set for the incident subcategory, filter by [Table] [is] [Incident] AND [Element] [is] [subcategory].
3. Check the box beside the choice set record to delete and select Delete from the Actions choice list below the list.
4. Click Delete in the confirmation window.
   All choices for the field are deleted.

Create a choice list for another field type
You can create a choice list for a field with another type, such as an integer, string, or reference field.
Role required: personalize_dictionary
You can use this configuration to standardize data entry and limit available options for a field while still maintaining the original field type.
1. Navigate to System Definition > Dictionary.
2. Open the dictionary entry for the field.

   Note: Reference fields with a large number of records in the reference table cannot be converted to look like choice fields. A reference field with too many records reverts to looking like a reference field.
3. Change the Choice value to Dropdown with --- None --- or Dropdown without --- None --- (must specify a default value).
4. Right-click the form header and select Save.
5. Click Create Choice List.
   • The Choices related list appears on the dictionary entry form.
   • If records on the table contains data for the field, a choice list value for each unique field value is created. For example, if three records exist on the table and each record has a unique value in the field, then three choices are created.
   • If no data exists in the field, a choice list value of --- New choice --- is created.

Display invalid choice list values
By default, inactive or invalid choice list values appear in blue text instead of black. You can disable the color indicator for invalid choices.
Role required: admin
In the following example, the Network category has been deactivated, so it appears in blue for records that still contain the inactive value.
1. Navigate to System Properties > UI Properties.
2. Clear the check box for the Display missing choice list entries property.

**Add search option to a choice field**
Add a search field to choice fields that have a long list of options.

Role required: admin

1. Navigate to a form that contains choice fields. For example, incident.
2. From a choice field on the form, for example State, right-click the field and select Configure Dictionary.
3. Switch to the advanced view for the dictionary entry form using the context menu by navigating to View > Advanced.
4. In the Attributes field, type is_searchable_choice=true. If there are other entries in the attributes field, use a comma to separate the entries.
5. Update the Dictionary Entry form and reload the page containing the choice list.

The choice list contains a search field that users can use to filter the list of choices.
Condition field types

A condition field specifies when to run business logic such as a business rule or workflow.

There are two types of condition field.

<table>
<thead>
<tr>
<th>Condition field type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition string</td>
<td>A text field that accepts a plain JavaScript condition statement. The system validates the condition syntax for correctness before an update.</td>
</tr>
<tr>
<td>Conditions</td>
<td>A field that adds a condition builder to a form. Condition builders require specifying a dependent field whose values the system uses to display choice list options. Typically, the dependent field is the Table field.</td>
</tr>
</tbody>
</table>

The system evaluates both types of condition field to determine if the conditions are true or false. When true, the system runs the business logic. When false, the system ignores the business logic.

To find dictionary attributes that affect condition fields, see Dictionary attributes.

Add the condition count to a condition field

The condition count widget can be activated on condition fields to display a preview of the records that would meet the current set of conditions. For fields where the condition count is activated, the number of records that match the conditions will automatically display. The count refreshes if the field the condition field depends on, such as Table, is changed. If the Table field is left blank, the widget is hidden.

Role required: personalize_dictionary

1. Right-click the field label and select Configure Dictionary.
2. Add show_condition_count=true to the Attributes field.
3. Submit.

In this example, a condition is run on the Incident table to look for incidents where Category is Network:

Condition count

The list shows that there are 112 records with Network as its category.

To refresh the preview, click the update count icon ( ).

To view details of the results, click the number of records to open the list view of the results:
Condition count results

Update a conditions field to use condition builder v2

In UI16, you can update a conditions field to display the version 2 condition builder.

Role required: admin

You add a dictionary attribute to the Conditions field to enable condition builder version 2 (v2).
Condition builder v2 configured in Approval Rules form

1. Open the form with the condition builder to configure.
2. Right-click the **Conditions** label and click **Configure Dictionary**.
3. In the **Attributes** field, enter `condition_builder=v2`.
   If attributes exist, add this string at the end separated by a comma.
4. Click **Update**.
   The form reloads with the v2 version of the condition builder.

Database field type

Several field types are available in the system.

This table shows field types and corresponding MySQL database types. Typically, it isn’t necessary to perform any actions at the database level. To learn about changing a field type, see System dictionary.
### Database field types

<table>
<thead>
<tr>
<th>Field types</th>
<th>Options</th>
<th>Dictionary XML type</th>
<th>MySQL DB type</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>small</td>
<td>string</td>
<td>VARCHAR(40)</td>
</tr>
<tr>
<td>String</td>
<td>medium</td>
<td>string</td>
<td>VARCHAR(100)</td>
</tr>
<tr>
<td>String</td>
<td>large</td>
<td>string</td>
<td>MEDIUMTEXT</td>
</tr>
<tr>
<td>String</td>
<td>extralarge</td>
<td>string</td>
<td>MEDIUMTEXT</td>
</tr>
<tr>
<td>Decimal</td>
<td></td>
<td>decimal</td>
<td>Decimal (15,2)</td>
</tr>
<tr>
<td>Integer</td>
<td></td>
<td>integer</td>
<td>Integer</td>
</tr>
<tr>
<td>True-False</td>
<td></td>
<td>boolean</td>
<td>TINYINT(1)</td>
</tr>
<tr>
<td>Date</td>
<td></td>
<td>glide_date</td>
<td>DATE</td>
</tr>
<tr>
<td>Date-Time</td>
<td></td>
<td>glide_date_time</td>
<td>DATETIME</td>
</tr>
<tr>
<td>Time</td>
<td></td>
<td>glide_time</td>
<td>DATETIME</td>
</tr>
<tr>
<td>Duration</td>
<td></td>
<td>glide_duration</td>
<td>DATETIME</td>
</tr>
<tr>
<td>Choice</td>
<td></td>
<td>string</td>
<td>VARCHAR(40)</td>
</tr>
<tr>
<td>Suggestion</td>
<td></td>
<td>string</td>
<td>VARCHAR(40)</td>
</tr>
<tr>
<td>Journal</td>
<td></td>
<td>journal</td>
<td>MEDIUMTEXT</td>
</tr>
<tr>
<td>Reference</td>
<td>&lt;reference table&gt;</td>
<td>reference</td>
<td>VARCHAR(32)</td>
</tr>
<tr>
<td>List</td>
<td></td>
<td>glide_list</td>
<td>MEDIUMTEXT</td>
</tr>
<tr>
<td>Url</td>
<td></td>
<td>url</td>
<td>MEDIUMTEXT</td>
</tr>
<tr>
<td>Image</td>
<td></td>
<td>user_image</td>
<td>VARCHAR(40)</td>
</tr>
<tr>
<td>Due-Date</td>
<td></td>
<td>due_date</td>
<td>DATETIME</td>
</tr>
</tbody>
</table>

### Dictionary entry data types

You can only change a dictionary entry's data type when the change does not result in data loss. Use the following guidelines to change a dictionary entry's data type.

**Valid data type changes**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The field is empty in all table records.</td>
<td>None. You can convert an empty field from any data type to another without restriction.</td>
</tr>
<tr>
<td>The table contains existing data for the field.</td>
<td>You can only convert between logical data types that map to the same physical data type in the database. For example, you can convert a <em>glide duration</em> to a <em>glide datetime</em> since both logical data types map to the DATETIME physical data type in the database.</td>
</tr>
<tr>
<td>Condition</td>
<td>Restrictions</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>The field is a string field you are converting to another type of string field.</td>
<td>You can change between string-based data types as long as length changes do not cause any data loss from truncation. For example, you can change from a MEDIUM database type to a VARCHAR(100) database type if none of the existing data is greater than 100.</td>
</tr>
<tr>
<td>The field is a string field you are converting to a globally unique ID (GUID).</td>
<td>You can only convert a string field to a GUID if all of the exiting data in the field are already <strong>Sys ID</strong> values.</td>
</tr>
<tr>
<td>The field is a GUID field you are converting to a string field.</td>
<td>None. You can convert a GUID field to a string field without restriction.</td>
</tr>
</tbody>
</table>

**Document ID field**

You can create document ID fields to reference any record on any table.

Role required: personalize_dictionary

In comparison, a reference field references a record on a specific table. To reference records from any table, two fields need to work together—one to store the table reference and another to store the record reference.

You can select the document ID type when creating a new field.

1. Navigate to the form view for the table.
2. Right-click the header and select **Configure > Form Layout**.
3. Create a field to store the table name and click **Add**.
   - **Name**: any label (for example, **Model table**)
   - **Type**: String
4. Create a field to store the record reference and click **Add**.
   - **Name**: label for your document ID field (for example, **Model ID**)
   - **Type**: Document ID
5. Click **Save**.
6. Right-click the form header and select **Configure > Dictionary**.
7. Open the dictionary entry for the document ID field.
8. Under **Related Links**, click **Advanced view**.
9. In the **Dependent** field, enter the column name of the table reference field (for example, **u_model_table**).
10. Optional: In **Attributes**, add the **show_all_tables** dictionary attribute to display system tables.
11. Click **Update**. When users click the reference lookup for the document ID field, a dialog appears that allows them to select the table and then the record. The sys_id of the selected record is stored in the document ID field and the table name is stored in the table reference field.
12. Optional: **Configure the form** to remove the table reference field.

![Select the document dialog](image-url)
Function field

Create function fields and scripts in the Now Platform to perform common database transformations and calculations. Regular fields store a value in the database. Instead of storing data, a function field displays the results of a database query. Function fields do not have an associated database column. Instead, function fields generate a value based on simple computations of other fields and constants. They can be used like any other fields in the system: in forms, lists, query conditions, reports, and so on.

Use case

You want to identify all incidents with a probably useless short description of fewer than 10 characters.

Instead of querying all records to determine which record meets a given criteria, create a function field or function script that retrieves only the records that meet the criteria.

For a simple computation, it is better to use a function field or function script rather than store a computed value. The value is always calculated on retrieval. Another benefit of using function fields is that the database server performs the transformation rather than the application node.

Function fields versus calculated fields

The values of the calculated fields are stored in the database. The values of function fields or function scripts are not stored in the database, but are calculated at the time of retrieval. Function field values are always up to date.

Function fields versus business rules

Use function fields or scripts when business logic is based on a simple transformation of one or more existing fields. Function fields and scripts let you implement business logic without storing and maintaining the result of a transformation.

Function fields versus filters, query strings, and Rhino

Rather than calling Rhino to perform string transformations, you can use a function field or function script to perform the transformations for you. Function fields and function scripts are more efficient and result in up-to-date values that do not have to be stored or maintained.

Function field limitations

Because function field calculations are not stored in the database, some operations are not relevant.

- Function fields cannot be directly audited or indexed.

  Note: To index a function field as if it were a regular field, make sure the individual fields used by the function are indexed. Or for best performance, make sure that there is a composite index including all fields that are used in the function.

- Function fields cannot be encrypted, since a function field value is never stored in the database.
- Function fields cannot be converted to regular fields or vice versa.
- Function fields in reportiFunction fields that you create in the Reporting UI do not support dot-walking. For more information, see Configure function fields in Reporting.se views do not support function fields.
- Security is evaluated on the components of the function and on the calculated value of the field. When used in visualizations, sections that contain information that the user is not allowed to see are hidden from the user.
- Datediff is not supported in the Kagami database.
• Field function names must be unique.

**Defining platform functions**

Platform functions can be defined in two ways:

1. Use the following application programming interfaces (APIs) to build and use functions in a script.

**Function APIs**

<table>
<thead>
<tr>
<th>APIs</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scoped GlideDBFunctionBuilder</td>
<td>Construct the function to perform a SQL operation.</td>
</tr>
<tr>
<td>GlideRecord - addFunction(Object function)</td>
<td>Apply the function to a GlideRecord.</td>
</tr>
</tbody>
</table>
2. Create a field that holds the function definition, as shown in the following example.
The Dictionary Entry [sys_dictionary] form has a **Function field** check box which specifies that the field runs a function rather than stores a value.

### glidefunction operations

Function fields can perform the following operations using the `glidefunction:<operation>` syntax. When providing a field as an argument, you can dot-walk to related fields. For example, `cmdb_ci.name`.

#### Function field operations

The Function field operations table contains columns for the names of function field operations, a detailed description of what the operation does, and an example that includes both code and what the code returns.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>add()</td>
<td>Takes two number fields as input, adds them, and returns the results as a field value. This function also takes numerical values for either input. Place numerical values in single or double quotation marks.</td>
<td><code>glidefunction:add(child_incidents, parent_incident)</code>&lt;br&gt;Returns 6 if the incident has five child incidents and one parent incident.&lt;br&gt;Possible return types: Decimal, Floating Point Number, Large Whole Number, Whole Number</td>
</tr>
<tr>
<td>subtract()</td>
<td>Takes two number fields as input, subtracts the second from the first, and returns the result as a field value. This function also takes numerical values for either input. Place numerical values in single or double quotation marks.</td>
<td><code>glidefunction:subtract(u_num1, u_num2)</code>&lt;br&gt;Returns 2 if num1 = 8 and num_2 = 6.&lt;br&gt;Possible return types: Decimal, Floating Point Number, Large Whole Number, Whole Number</td>
</tr>
<tr>
<td>multiply()</td>
<td>Takes two number fields as input, performs the multiplication, and returns the results as a field value. This function also takes numerical values for either input. Place numerical values in single or double quotation marks.</td>
<td><code>glidefunction:multiply(u_num1, u_num2)</code>&lt;br&gt;Returns 48 if num1 = 8 and num_2 = 6.&lt;br&gt;Possible return types: Decimal, Floating Point Number, Large Whole Number, Whole Number</td>
</tr>
<tr>
<td>divide()</td>
<td>Takes two number fields as input, divides the first by the second, and returns the result as a field value. This function also takes numerical values for either input. Place numerical values in single or double quotation marks.</td>
<td><code>glidefunction:divide(u_num2,u_num1)</code>&lt;br&gt;Returns 5 if num2 = 10 and num1 = 2.&lt;br&gt;Possible return types: Decimal, Floating Point Number, Large Whole Number, Whole Number</td>
</tr>
<tr>
<td>Operation</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>concat()</td>
<td>Takes any number of comma-separated fields and constants as input, concatenates the input, and returns a single string as a field value.</td>
<td><code>glidefunction:concat(incident_number, '/', short_description)</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Returns &quot;INC0001 / My client needs a new laptop.&quot; if the value of the number field is 'INC0001' and the short_description is 'My client needs a new laptop'.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Return type: Text</td>
</tr>
<tr>
<td>datediff()</td>
<td>Takes two date/time fields as input, calculates the difference between the dates in days, minutes, and seconds, and returns the results as a duration field value.</td>
<td><code>glidefunction:datediff(closed_at, sys_created_on)</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Returns the duration of an incident from the creation date to the close date. Example result: 10 days, 8 hours 23 minutes 11 seconds</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Return type: Duration</td>
</tr>
<tr>
<td>dayofweek()</td>
<td>Takes two arguments: A date field and a constant of either '1' (week starts on Sunday) or '2' (week starts on Monday). Returns the results as an integer value that represents the day of the week.</td>
<td><code>glidefunction:dayofweek(resolved_at, '1')</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>If resolved_at occurs on a Wednesday, returns 4 if the integer is 1 and returns 3 if the integer is 2.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Return type: Whole number</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This function is not available for Kagami.</td>
<td></td>
</tr>
<tr>
<td>length()</td>
<td>Takes a string field as input, calculates the field length in characters, and returns the results as a field value.</td>
<td><code>glidefunction:length(short_description)</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Returns 37 if short_description = &quot;This application is performing a test&quot;.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Return type: Whole number</td>
</tr>
<tr>
<td>coalesce()</td>
<td>Takes any number of comma-separated fields as input and returns the first non-empty value.</td>
<td><code>glidefunction:coalesce(closed_at, resolved_at, sys_updated_on)</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>If the value of closed_at is empty, the function returns the value of resolved_at. If the value of resolved_at is also empty, the function returns the value of sys_updated_on.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Return type: Text</td>
</tr>
<tr>
<td>Operation</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| position()   | Takes two text fields or two text fields and a whole number as input. One or both of the text fields can also be strings.                                                                                                          | 1. `glidefunction:position('e', short_description)`  
If the value of the `short_description` field is "This computer is performing an upgrade", returns 12.  
2. `glidefunction:position('e', short_description, '14')`  
If the value of the `short_description` field is "This computer is performing an upgrade", returns 19.  
Return type: Whole number                                                                                                                                                         |
| substring()  | Takes a text field and two whole numbers as input. Returns the first instance of a string that starts at the position of the first whole number and is the length of the second.                                                      | `glidefunction:substring(short_description, '7', '2')`  
If the value of the `short_description` field is 'We're going to the store', returns 'go'.  
Return type: Text                                                                                                                                                                    |

### Create a function field to perform database functions

Create a field that displays the results of a database function, such as a mathematical operation, field length computation, or day of the week calculation.

Role required: personalize_dictionary or admin.

1. Navigate to **System Definition > Dictionary**.  
2. Click **New**.  
3. Select **Function field**.  
4. Fill in these fields on the form.

#### Fields for function fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>Table to which the function field is added.</td>
</tr>
<tr>
<td>Type</td>
<td>Species the type of field: string, number, date, and so on.</td>
</tr>
<tr>
<td>Column label</td>
<td>Defines the label for the column.</td>
</tr>
<tr>
<td>Column name</td>
<td>Defines the name of the column. Created automatically based on <strong>Column label</strong>.</td>
</tr>
<tr>
<td>Max length</td>
<td>Defines the maximum length of the return value.</td>
</tr>
</tbody>
</table>
### Field

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function field</td>
<td>If selected, creates a field that displays the results of a database function, such as a mathematical operation, field length computation, or day of the week calculation. Once the new function record is saved, you cannot clear the check box to make the field a regular field.</td>
</tr>
<tr>
<td>Function definition</td>
<td>Defines the function that the field performs. Starts with <code>glidefunction:</code> followed by the operation to be performed (for example, <code>concat</code>), followed by function parameters. Constants must be enclosed in single quotes. For example, the following function definition creates a field that shows the short description, followed by a space, followed by the caller name: <code>glidefunction:concat(short_description, ' ', caller_id.name)</code></td>
</tr>
</tbody>
</table>

**Note:** Function parameters support dot walking. See Dot-walking to data in related tables.

5. Click **Submit**. You return to the Dictionary Entry `[sys_dictionary]` table.
6. Navigate to the table to which you added the function field.
7. Add the function field to the list. See Configure items on forms or in lists using a list collector.

Use the function field like any other field. For example, add it to a form, use it in a filter, or use it in the condition builder.

If the function definition is invalid, instead of the expected value you receive the message **Invalid function** if the function field is a string type field, or an empty value for other field types.

### HTML field type

The HTML editor provides WYSIWYG (what you see is what you get) functionality and HTML source mode editing. Administrators can customize some of the functionality associated with HTML fields.

The HTML editors available depend on your version of the UI.

**UI support for available HTML editors**

<table>
<thead>
<tr>
<th>HTML editor</th>
<th>UI support</th>
</tr>
</thead>
<tbody>
<tr>
<td>TinyMCE version 4</td>
<td>UI16, UI15</td>
</tr>
<tr>
<td>htmlArea (legacy)</td>
<td>Basic support in UI16</td>
</tr>
</tbody>
</table>

Knowledge articles, service catalog item descriptions, release documentation, and HTML content blocks are common examples of HTML fields.

**Note:** The TinyMCE editor does not support converting Microsoft Word Shapes into HTML.
While HTML fields can be added to split forms, HTML fields are not intended for this use and can behave unexpectedly due to the limited available width in split pane forms.

If accessibility is enabled, a help icon appears with the HTML field. The help icon indicates how to use keys to access and escape the HTML field toolbar.

**Configure a field editor for the HTML field**

You can configure HTML fields to use TinyMCE or the legacy HtmlArea editor. This editor provides better stability and more editing functions than the legacy HtmlArea editor.

Role required: admin

There are two options for HTML editors.

- TinyMCE: A What You See Is What You Get (WYSIWYG) field that displays text as readers would see it on the screen. TinyMCE is the default editor.
- HtmlArea: The legacy editor, which offers a more basic WYSIWYG interface as well as a mode that shows only HTML markup.

1. Navigate to **System Properties > UI Properties**.
2. Locate the property called **HTML field editor to use (glide.ui.html.editor)**.
3. Select **TinyMCE** or **HtmlArea**.
4. Click **Save**.

**Configure the HTML toolbar**

When HTML fields are configured to use the HTML editor, follow this procedure to configure which buttons are available on the toolbar.

Role required: admin

1. Navigate to **System Properties > UI Properties**.
2. Locate the appropriate properties based on your version of the HTML editor.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TinyMCE</td>
<td>glide.ui.html.editor.v4.toolbar.line1 and glide.ui.html.editor.v4.toolbar.line2</td>
</tr>
<tr>
<td>HtmlArea</td>
<td>glide.ui.html.toolbar</td>
</tr>
</tbody>
</table>

3. Enter or remove buttons for each toolbar as a comma-separated list without spaces.

For the TinyMCE toolbar, use the following buttons. Use a vertical bar ("|") to add a section separator.

**TinyMCE button options**

<table>
<thead>
<tr>
<th>Button purpose</th>
<th>Accepted button names</th>
</tr>
</thead>
<tbody>
<tr>
<td>Formatting</td>
<td>newdocument, bold, italic, underline, strikethrough, justyleft, justifycenter, justifyright, justifyfull, formatselect, fontselect, fontsizeelect, bullist, numlist, outdent, indent, blockquote, forecolor, removeformat, backcolor, sub, sup</td>
</tr>
<tr>
<td>Table functions</td>
<td>tablecontrols</td>
</tr>
<tr>
<td>Editing</td>
<td>cut, copy, paste, pastetext, search, replace, undo, redo</td>
</tr>
</tbody>
</table>
### Button purpose | Accepted button names
--- | ---
Extended functions | link, unlink, cleanup, code, hr, visualaid, charmap, image, media, preview, spellchecker, fullscreen (not supported by Internet Explorer)
The **spellchecker** tool is not supported in UI16 or UI15.

For the htmlArea toolbar, use the following buttons. Use *separator* to add a section separator.

#### htmlArea button options

| Button purpose | Accepted button names |
--- | ---|
Formatting | formatblock, fontname, fontsize, bold, italic, underline, justifyleft, justifycenter, justifyright, justifyfull, insertorderedlist, insertunorderedlist, outdent, indent, forecolor, hilitecolor |
Editing | copy, paste, undo |
Extended functions | createlink, inserthorizontalrule, insertimage, insertvideo, inserttable, htmlmode |

4. **Click** **Save**.

![TinyMCE toolbar](image1)

![htmlArea toolbar](image2)

**Configure TinyMCE to allow deprecated tags**

You can set a dictionary attribute on a TinyMCE field to allow the use of deprecated HTML tags, such as `<b>` and `<i>`. By default, TinyMCE uses the `<strong>` and `<em>` tags for bold and italic formatting.

Role required: personalize_dictionary or admin

After you set the dictionary attribute, use code view to manually enter deprecated tags. The editor does not validate any tags you enter manually, for example, if you type an incorrect character.

1. Navigate to the form with an HTML field that uses TinyMCE.
2. Right-click the HTML field label and select **Configure dictionary**.

3. In the **Attributes** field, enter `tinymce_allow_all=true`, separated by a comma if needed. If other attributes are already listed, use a comma as a separator.

4. Click **Update**.

Configure TinyMCE to allow JavaScript in URLs
You can set a dictionary attribute on a TinyMCE field to allow the use of JavaScript in a URL.

Role required: personalize_dictionary or admin

1. Navigate to the form with an HTML field that uses TinyMCE.
2. Right-click the HTML field label and select Configure dictionary.

3. In the Attributes field, enter tinymce_allow_script_urls=true, separated by a comma if needed. If other attributes are already listed, use a comma as a separator.

4. Click Update.

**Formatting icons for the HTML field editors**

The formatting table displays how to control the way text appears.

The following table displays icons that are available in the TinyMCE and the htmlArea editors. Names marked with an asterisk (*) are not available with the htmlArea editor.

<table>
<thead>
<tr>
<th>htmlArea icon</th>
<th>TinyMCE icon</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>B</td>
<td>Bold</td>
<td>Applies bold formatting to the selected text or current word.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Keyboard shortcut: CTRL + B</td>
</tr>
<tr>
<td>I</td>
<td>I</td>
<td>Italic</td>
<td>Applies italics formatting to the selected text or current word.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Keyboard shortcut: CTRL + I</td>
</tr>
<tr>
<td>U</td>
<td>U</td>
<td>Underline</td>
<td>Applies underline formatting to the selected text or current word.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Keyboard shortcut: CTRL + U</td>
</tr>
<tr>
<td>htmlArea icon</td>
<td>TinyMCE icon</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------</td>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Align Right</strong></td>
<td><img src="image" alt="Align Right Icon" /></td>
<td><strong>Align Right</strong></td>
<td>Applies right alignment to the current paragraph. Code reference: <code>text-align:right</code></td>
</tr>
<tr>
<td><strong>Align Center</strong></td>
<td><img src="image" alt="Align Center Icon" /></td>
<td><strong>Align Center</strong></td>
<td>Applies center alignment to the current paragraph. Code reference: <code>text-align:center</code></td>
</tr>
<tr>
<td><strong>Align Left</strong></td>
<td><img src="image" alt="Align Left Icon" /></td>
<td><strong>Align Left</strong></td>
<td>Applies left alignment to the current paragraph. Code reference: <code>text-align:left</code></td>
</tr>
<tr>
<td><strong>Justify</strong></td>
<td><img src="image" alt="Justify Icon" /></td>
<td><strong>Justify</strong></td>
<td>Applies justified alignment, which stretches the lines to equal width, to the current paragraph. Code reference: <code>text-align:justify</code></td>
</tr>
<tr>
<td><strong>Format</strong></td>
<td><img src="image" alt="Format Icon" /></td>
<td><strong>Format</strong></td>
<td>Applies a paragraph style to the current paragraph, such as Paragraph, Heading 1, and Preformatted.</td>
</tr>
<tr>
<td><strong>Font Family</strong></td>
<td><img src="image" alt="Font Family Icon" /></td>
<td><strong>Font Family</strong></td>
<td>Applies a font family to the selected text or current word.</td>
</tr>
<tr>
<td><strong>Font Size</strong></td>
<td><img src="image" alt="Font Size Icon" /></td>
<td><strong>Font Size</strong></td>
<td>Applies a font size to the selected text or current word.</td>
</tr>
<tr>
<td><strong>Insert/Remove Bulleted List</strong></td>
<td><img src="image" alt="Insert/Remove Bulleted List Icon" /></td>
<td><strong>Insert/Remove Bulleted List</strong></td>
<td>Applies or removes unordered list tags for the selected paragraphs. Click the arrow beside the button to select a different bullet type.</td>
</tr>
<tr>
<td><strong>Insert/Remove Numbered List</strong></td>
<td><img src="image" alt="Insert/Remove Numbered List Icon" /></td>
<td><strong>Insert/Remove Numbered List</strong></td>
<td>Applies or removes ordered list tags for the selected paragraphs. Click the arrow beside the button to select a different number type.</td>
</tr>
</tbody>
</table>
### htmlArea icon

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decrease Indent</td>
<td>Removes indentation from the current or selected paragraphs (removes 30px of left padding; padding cannot be less than 0). Code reference: padding-left</td>
</tr>
<tr>
<td>Increase Indent</td>
<td>Applies indentation to the current or selected paragraphs (adds 30px of left padding). Code reference: padding-left</td>
</tr>
<tr>
<td>Select Text Color</td>
<td>Applies font color to the current word or selected text. Click the button to use the current color, or click the arrow next to the button to view more colors. Click More Colors... to view various color options and the hexadecimal codes.</td>
</tr>
<tr>
<td>Select Background Color</td>
<td>Applies background color to the current word or selected text. Click the button to use the current color, or click the arrow next to the button to view more colors. Click More Colors... to view various color options and the hexadecimal codes.</td>
</tr>
</tbody>
</table>

### Extended functions

**Extended functions**
The extended functions available for working with HTML content.

### Icon

<table>
<thead>
<tr>
<th>Icon</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Link Icon" /></td>
<td>Insert/Edit Link</td>
<td>Configures a link for the selected text. Define the link URL, title (additional information that appears in the tooltip), and the target (same window or new window or tab). Code reference: <code>&lt;a&gt;</code></td>
</tr>
<tr>
<td>Icon</td>
<td>TinyMCE v4 Icon</td>
<td>Name</td>
</tr>
<tr>
<td>------</td>
<td>----------------</td>
<td>------</td>
</tr>
<tr>
<td><img src="image" alt="Remove link" /></td>
<td><img src="image" alt="Remove link" /></td>
<td>Remove link*</td>
</tr>
<tr>
<td><img src="image" alt="Cleanup Messy Code" /></td>
<td><img src="image" alt="Cleanup Messy Code" /></td>
<td>Cleanup Messy Code*</td>
</tr>
<tr>
<td><img src="image" alt="Edit HTML Source" /></td>
<td><img src="image" alt="Edit HTML Source" /></td>
<td>Edit HTML Source</td>
</tr>
<tr>
<td><img src="image" alt="Insert Horizontal Line" /></td>
<td><img src="image" alt="Insert Horizontal Line" /></td>
<td>Insert Horizontal Line</td>
</tr>
<tr>
<td><img src="image" alt="Toggle Invisible Elements" /></td>
<td><img src="image" alt="Toggle Invisible Elements" /></td>
<td>Toggle Invisible Elements*</td>
</tr>
<tr>
<td><img src="image" alt="Insert Special Character" /></td>
<td><img src="image" alt="Insert Special Character" /></td>
<td>Insert Special Character*</td>
</tr>
<tr>
<td><img src="image" alt="Insert/Edit Image" /></td>
<td><img src="image" alt="Insert/Edit Image" /></td>
<td>Insert/Edit Image</td>
</tr>
<tr>
<td><img src="image" alt="Insert/Edit Embedded Media" /></td>
<td><img src="image" alt="Insert/Edit Embedded Media" /></td>
<td>Insert/Edit Embedded Media</td>
</tr>
<tr>
<td><img src="image" alt="Spell Checker" /></td>
<td><img src="image" alt="Spell Checker" /></td>
<td>Spell Checker</td>
</tr>
<tr>
<td>Icon</td>
<td>TinyMCE v4 Icon</td>
<td>Name</td>
</tr>
<tr>
<td>------</td>
<td>-----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>![Preview Icon]</td>
<td></td>
<td>Preview*</td>
</tr>
<tr>
<td>![Full Screen Mode Icon]</td>
<td></td>
<td>Toggle Full Screen Mode*</td>
</tr>
</tbody>
</table>

*These options are not available with htmlArea.

**Editing functions in TinyMCE**

Several editing functions are built into TinyMCE.

You can add more edit functions to TinyMCE v4 using the `glide.ui.html.editor.toolbar.line1` and `glide.ui.html.editor.toolbar.line2` properties located on the UI Properties page. For more information on configuring the edit functions, see Configure the HTML toolbar.

**Editing functions**

<table>
<thead>
<tr>
<th>Icon</th>
<th>TinyMCE v4 Icon</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Cut Icon]</td>
<td></td>
<td>Cut*</td>
<td>Cuts the selected text. Not supported in all browsers; use keyboard shortcut. Keyboard shortcut: CTRL + X</td>
</tr>
<tr>
<td>![Copy Icon]</td>
<td></td>
<td>Copy*</td>
<td>Copies the selected text. Not supported in all browsers; use keyboard shortcut. Keyboard shortcut: CTRL + C</td>
</tr>
<tr>
<td>![Paste Icon]</td>
<td></td>
<td>Paste*</td>
<td>Pastes the selected text. Not supported in all browsers; use keyboard shortcut. Keyboard shortcut: CTRL + V</td>
</tr>
<tr>
<td>![Paste as Plain Text Icon]</td>
<td></td>
<td>Paste as Plain Text*</td>
<td>Enables paste as plain text without source formatting.</td>
</tr>
<tr>
<td>Icon</td>
<td>TinyMCE v4 Icon</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>----------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td><img src="image" alt="Paste from Word" /></td>
<td></td>
<td>Paste from Word*</td>
<td>Opens a new window that allows you to copy and paste content from Microsoft Word into the HTML field.</td>
</tr>
<tr>
<td><img src="image" alt="Find" /></td>
<td></td>
<td>Find*</td>
<td>Allows you to locate text strings in the HTML field. Search above (up) or below (down) the cursor location.</td>
</tr>
</tbody>
</table>
| ![Find/Replace](image) |              | Find/Replace* | Allows you to replace the next (Replace) or all (Replace All) occurrences of a text string in the HTML field.  
Keyboard shortcuts: CTRL + F, Cmd + F |
| ![Undo](image) | ![Redo](image) | Undo* | Reverts the previous edit. |
| ![Redo](image) |              | Redo* | Reapplies the last reverted edit. |

*These options are not available with htmlArea.*
### Table functions in TinyMCE

TinyMCE version 4 uses menus and menu selections to create and edit tables.

#### TinyMCE version 4

<table>
<thead>
<tr>
<th>UI element</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table menu</td>
<td>Click the table icon ( ) to access the TinyMCE version 4 table menu. Use the table menu to:</td>
</tr>
<tr>
<td></td>
<td>• Insert or delete a table</td>
</tr>
<tr>
<td></td>
<td>• Modify table properties</td>
</tr>
<tr>
<td></td>
<td>• Add, move, or delete rows and columns</td>
</tr>
<tr>
<td></td>
<td>• Modify row and column properties</td>
</tr>
<tr>
<td></td>
<td>• Split and merge cells</td>
</tr>
</tbody>
</table>

**Table insert grid**

To insert a table in the HTML field, click **Insert table** and highlight squares in the grid to represent the desired number of rows and columns. Click the last highlighted square to insert the table.

After you insert the table, you can modify the size by clicking and dragging the handles at the table edges.
From the table menu, click **Table properties** to open the Table properties dialog box. From this box you can take any of the following actions.

- **General tab:**
  - Set table width and height
  - Set cell spacing and padding
  - Enable borders and captions
  - Set the table alignment

- **Advanced tab:**
  - Configure the table style
  - Select the border color
  - Select the background color
<table>
<thead>
<tr>
<th>UI element</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cell properties</strong></td>
<td>With the cursor in the desired table cell, open the table menu and click <strong>Cell properties</strong>. From this box you can set the following properties for table cells.</td>
</tr>
<tr>
<td>General</td>
<td>• General tab:</td>
</tr>
<tr>
<td></td>
<td>• Width and height</td>
</tr>
<tr>
<td></td>
<td>• Type and scope</td>
</tr>
<tr>
<td></td>
<td>• Horizontal and vertical alignment</td>
</tr>
<tr>
<td>Advanced</td>
<td>• Advanced tab</td>
</tr>
<tr>
<td></td>
<td>• Configure the cell style</td>
</tr>
<tr>
<td></td>
<td>• Select the border color</td>
</tr>
<tr>
<td></td>
<td>• Select the background color</td>
</tr>
</tbody>
</table>

| **Row properties** | With the cursor in a table cell in the desired row, open the table menu and click **Row properties**. From this box you can set the following properties for rows. |
| General | • Row type |
| | • Alignment |
| | • Height |
| Advanced | • Advanced tab |
| | • Configure the row style |
| | • Select the border color |
| | • Select the background color |
You can also paste tables into HTML fields from table-based editors.

**Customize TinyMCE attributes**

Change TinyMCE toolbars and the default height of HTML fields to customize your journal field experience.

Add or remove TinyMCE attributes from the default TinyMCE toolbar. The TinyMCE attributes are applied to TinyMCE toolbars in the platform and workspaces, or to specific plugins in a record or specific tables in a record. You can also apply an attribute to increase the height of HTML fields, enlarging the HTML field that agents work with.

**Change the TinyMCE default toolbar**

Set the toolbar items in your system properties to enable or disable throughout Workspace.

Role required: admin

1. Navigate to **System Properties > UI Properties**.
2. Locate the appropriate properties based on your UI version.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UI16 or UI15</td>
<td>(TinyMCE v.4.0.26) Configures the editing toolbar (first line) for HTML fields (glide.ui.html.editor.v4.toolbar.line1).&lt;br&gt;• (TinyMCE v.4.0.26) Configures the editing toolbar (second line) for HTML fields (glide.ui.html.editor.v4.toolbar.line2).</td>
</tr>
<tr>
<td>UI11</td>
<td>Configures the editing toolbar (first line) for HTML fields(glide.ui.html.editor.toolbar.line1).&lt;br&gt;• Configures the editing toolbar (second line) for HTML fields(glide.ui.html.editor.toolbar.line2).</td>
</tr>
</tbody>
</table>

3. Add or remove buttons for each toolbar.

**Note:**
- Separate attributes with commas.
- Use a vertical bar ("|") to add a section separator.

<table>
<thead>
<tr>
<th>Type</th>
<th>Button Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default buttons</td>
<td>bold italic underline undo redo fontselect fontsizeselect table forecolor backcolor link unlink image media code alignleft aligncenter alignright bullist numlist fullscreen</td>
</tr>
<tr>
<td>Type</td>
<td>Button Names</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Valid buttons</td>
<td>newdocument bold italic underline strikethrough alignleft aligncenter alignright align justify formatselect fontselect fontsizeselect table cut copy paste pastetext searchreplace bullist numlist outdent indent blockquote undo redo link unlink code forecolor backcolor removeformat hr visualblocks subscript superscript charmap image media fullscreen anchor toc codesample ltr rtl emoticons insertdatetime nonbreaking pagebreak print visualblocks visualchars cut copy</td>
</tr>
</tbody>
</table>

4. Click **Save**.

Change the TinyMCE toolbar for a specific table

Set the attributes in the TinyMCE dictionary to determine which TinyMCE attributes show in a specific table.

Role required: admin

1. In platform, select the record of an HTML field you want to change.
   For example, select an incident, problem, or knowledge record.
2. Right-click the field label (Article body) and select **Configure Dictionary**.

3. In Related Links, click **Advanced View**.

4. In the **Attributes** field, input `editor.toolbar.line1= or editor.toolbar.line2` followed by the plugin.

   **Note:** Separate attributes with a space.

5. Click **Update**.

Change TinyMCE plugins for a specific table

Set the attributes in the TinyMCE dictionary to enable or disable plugins in a specific HTML field.

Role required: admin

1. In platform, select the record of an HTML field you want to change.
   For example, select an incident, problem, or knowledge record.
2. Right-click the field label (Article body) and select **Configure Dictionary**.

3. In Related Links, click **Advanced View**.

4. In the **Attributes** field, input `editor.plugins=` followed by the plugin. For a list of plugins, click here.

   **Note:**
   - Include all toolbar items you want displayed and not just the toolbar items you want to add.
   - Separate plugins with a space.

5. Click **Update**.

Change the default height of an HTML field

Change the default height of a specific HTML field to expand the size of a journal field.

Role required: admin

HTML field height is configured per HTML field.

1. In platform, select the record of an HTML field you want to change.
   
   For example, select an incident, problem, or knowledge record.
2. Right-click the field label (Article body) and select **Configure Dictionary**.

3. In Related Links, click **Advanced View**.

4. In the **Attributes** field, enter `editor.height=X`.
   For example, `editor.height=250`

   **Note:**
   HTML fields can range from 72 to 2000. HTML fields are by default 64.

5. Click **Update**.

   **Highlight text in TinyMCE**
   On the bottom bar of TinyMCE, the path of HTML tags for the text at the cursor position is displayed.
   Click a tag in the path to highlight the text affected by the tag.

   **Insert a line break in the HTML editor**
   When you use the **Enter** key, the editor creates a paragraph element (`<p>`) tag, which appears as a double space.
   To enter a single-line space, use the **Shift + Enter** key combination, which inserts a line break (`<br>`) tag.
Add a table to the HTML field
This example uses HTML field controls to format a table in a knowledge article.

Table example html

To add the formatted table to a knowledge article:

1. Navigate to Knowledge > Edit and select the article to edit.
2. In the HTML field, position the cursor in the location for the table.
3. Click the table icon, click **Insert table**, and then select the number of rows and columns.

4. Complete the following steps to edit the table properties.
   a) Position your cursor in the table, click the table icon, and select **Table properties**.
   b) Enter the following values on the **General** tab.
      - Width: 75%
      - Cell spacing: 3
      - Cell padding: 3
      - Border: 1
      - Alignment: Left
   c) On the **Advanced** tab, click the text field next to **Border color** and enter **Gray**.
      The color picker box to the right turns gray to indicate the color that you entered. You can also click the box and select the color in the palette.
   d) Click **Ok**.

5. Complete the following steps to update the header table row.
   a) Select the cells in the first table row, click the table icon, and select **Row > Row properties**.
   b) Enter the following values on the **General** tab.
      - Row type: Header
      - Alignment: Center
   c) On the **Advanced** tab, enter `#87cef` in the text box beside **Background color** to set it to a light blue.
   d) Click **Ok**.
6. To set cell properties, complete the following steps.
   a) Select all table cells in the first column except those cells in the header row, click the table icon, and select Cell > Cell properties.
   b) Enter the following values on the General tab.
      • H Align: Left
      • V Align: Top
   c) Click Ok.
   d) Repeat these steps for the table cells in the second column.

7. To set the background color of the middle row, complete the following steps.
   a) Position your cursor in the middle table row, click the table icon, and select Row > Row properties.
   b) On the Advanced tab, enter Silver in the text box beside Background color to set it to color #c0c0c0.
   c) Click Ok.

Repeat this procedure for every other table row.

8. To set column width, complete the following steps.
   a) Click the first column of the table, click the table icon, and select Cell > Cell properties.
   b) On the General tab, enter 30% in the Width text field.
   c) Click Ok.

9. Right-click the form header and click Save.
10. Enter data in the table cells and then save the article.

**Embed images in HTML fields**
You can use the HTML field image picker to embed images into HTML fields, and to add images to the image library.

Role required: the role necessary to update the record that contains the HTML field. For example, any user with a role can create a knowledge article and embed an image in it.

**Note:** Administrators and users with the image_admin role manage the image library at System UI > Images. See Storing images in the database.

1. Open the form that contains the HTML field.
2. Click the position where the image is to appear, or to modify an existing image, click the image.
3. Click the insert/edit image icon (🖼) on the HTML editor toolbar.
4. In the Insert/Modify image form, enter information in each field.

**Insert/Modify Image form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>Select the image type.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Image Library</strong>: Images stored in the db_image table. You can reuse images in the image library in multiple locations.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Attachment</strong>: Available in the current record only</td>
</tr>
<tr>
<td><strong>Image</strong></td>
<td>Begin typing a file name and select an image from the list, or click the reference lookup icon and select an image.</td>
</tr>
<tr>
<td></td>
<td>To upload a new image, click <strong>New</strong>, then <strong>Choose File</strong>, locate the image, and click <strong>Upload</strong>.</td>
</tr>
<tr>
<td></td>
<td>If you chose the <strong>Attachment</strong> type, click <strong>Choose File</strong>, locate the image, and click <strong>Attach</strong>.</td>
</tr>
<tr>
<td><strong>Tooltip</strong></td>
<td>Enter alternate text that appears when a user points to the image.</td>
</tr>
<tr>
<td><strong>Alt</strong></td>
<td>Enter alternate text that can be used to improve accessibility. For example, it could be used with a screen reader. If this field is left blank, it defaults to the text entered in the <strong>Tooltip</strong> field.</td>
</tr>
</tbody>
</table>

**Note:** To resize an embedded image, click the image. The sizing frame appears. Drag a sizing point until the image is the desired size. Corner points adjust the size proportionally. Depending on your browser, you may need to highlight the image before the sizing frame appears.

5. Optional: To provide additional control over the appearance of an image, click **Advanced options**.

**Advanced options**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Layout</strong></td>
<td>Select the image <strong>Alignment</strong> (default is <strong>Baseline</strong>) and enter the <strong>Border thickness</strong>.</td>
</tr>
<tr>
<td><strong>Spacing</strong></td>
<td>Enter the number of <strong>Horizontal</strong> and <strong>Vertical</strong> pixels around the image.</td>
</tr>
<tr>
<td><strong>Size</strong></td>
<td>Enter the <strong>Width</strong> and <strong>Height</strong> of the image (in pixels).</td>
</tr>
</tbody>
</table>

6. Click **OK**.

7. Optional: Paste an image into the HTML editor. To edit the image, save the entry then select the image. Click the insert/edit image icon and complete the form using the same tables for adding an image.

Pasted images are saved in the system as attachments.
Link to a website in HTML fields

You can insert a link to a website in an HTML field.

Role required: the role necessary to update the record that contains the HTML field. For example, any user with a role can create a knowledge article and link to a website in the article text.

1. Move the cursor to the position where the link is to appear.
2. Click the insert/edit link icon in the HTML toolbar.
3. Enter information in each field.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>Enter the URL for the link. Copying and pasting is usually the easiest method.</td>
</tr>
<tr>
<td>Text</td>
<td>Enter the text you want to display for the link.</td>
</tr>
<tr>
<td>Target</td>
<td>Select the target window for the URL.</td>
</tr>
</tbody>
</table>

For files, the **None (use implicit)** selection is generally the best choice. However, if you are linking to a complete web page, choose **New window (_blank)** so the browser opens the link in a new tab or window.

4. Click **OK** to insert the link into the field.

Embed videos in HTML fields

You can insert videos into HTML fields. You can also add videos to the video library using the HTML Insert/Modify Video form.

Role required: The role necessary to update the record that contains the HTML field. For example, any user with a role can create a knowledge article and embed a video in it.

The following file formats are supported in the base system.

- MPEG-4 video .mp4
- WebM Video .webm

The larger the file size, the longer it takes to download before the video starts. To reduce file size, you can reduce the bit rate, but doing so reduces the quality of the video. The following bit rates optimize download speed and video quality:

<table>
<thead>
<tr>
<th>Video resolution</th>
<th>Recommended bitrate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard definition (480p)</td>
<td>1.5–2.5 megabits per second (mbps)</td>
</tr>
<tr>
<td>High definition (720p)</td>
<td>3–5 mbps</td>
</tr>
<tr>
<td>High definition (1080p)</td>
<td>6–8 mbps</td>
</tr>
</tbody>
</table>

Internet Explorer and Safari have difficulty streaming videos uploaded to the database. Attach a file rather than embedding if you intend to use one of these browsers or an unsupported file type. For more information on attaching files, see [Add and manage attachments](#).
Note: Administrators and users with the image_admin role can manage the video library at System UI > Videos.

1. Open the form that contains the HTML field.
2. Click the position where the video is to appear, or to modify an existing video, click the video.
3. Click the insert/edit video icon on the HTML editor toolbar.
4. Enter information in each field.

### Insert/Modify Video

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select the video type.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Video Library</strong>: List of videos stored in the db_video table. You can reuse it.</td>
</tr>
<tr>
<td></td>
<td>• <strong>URL</strong>: from an external source</td>
</tr>
<tr>
<td></td>
<td>• <strong>Attachment</strong>: available in the current record only</td>
</tr>
<tr>
<td></td>
<td>For an attachment or video library file, select a video from the list or click New. For an external URL, enter the URL.</td>
</tr>
<tr>
<td>Size</td>
<td>Enter the <strong>Width</strong> and <strong>Height</strong> of the video in pixels.</td>
</tr>
</tbody>
</table>

5. Click OK.

**Define video file types for HTML fields**
You can define the types of video files that can be added to HTML fields.

Role required: image_admin

Users can add videos to HTML fields. By default, users can add one of the following types of videos to HTML fields: .mp4, .webm, and .swf video file types. You can inactivate video types that you do not want to allow users to add, or add new video types. .swf files are only minimally supported. .mp4 files might be limited by browser type.

Note: By default, the HTML Sanitizer removes videos from HTML fields. To allow video file types, see Embed videos in HTML fields

1. Navigate to System UI > Embed Object Types.
2. To deactivate a video type, set the **Active** field to false.
3. To add an additional video type, click New and complete the form.

Note: If you specify values for the Codebase or Pluginspage fields, which instruct the browser where to get the plugin, point to https pages to avoid warnings from Internet Explorer about unsecure content on the page.
Disable user access to the image library
By default, users can use and upload images to the image library from an HTML field. You can disable access to the image library from HTML fields.

Role required: admin

1. Navigate to System UI > UI Pages.
2. Select html_insert_image_dialog.
3. Locate the following lines of code in the HTML field and comment them out.

```xml
<g:evaluate var="jvar_use_dbimage">
  var imageGR = new GlideRecord('db_image');
  if(imageGR.isValid())
    imageGR.canRead();
</g:evaluate>

and

```xml
<j:if test="${jvar_write_dbimage}"
  <j:set var = "jvar_default_insert_image_type" value = "dbimage" />
  <g:ui_select_option text = "${gs.getMessage('Image Library')}" value = "dbimage" selected = "${jvar_default_insert_image_type}" />
</j:if>
```

4. Click Update.

To remove the Upload from URL option in the HTML editor, add a new property named glide.ui.html.image.allow_url and set the Value to false.

Paste content into the HTML editor
Paste content from a desktop application to the HTML editor. Content might not paste the same from every application.

Role required: admin

1. Navigate to an HTML field. For example, the Text field of a Knowledge article.
2. Paste in content from another application.
   Google Chrome and Mozilla Firefox do not support paste using the Paste icon. Use the command/control+V keyboard shortcut instead.
3. From the paste formatting options dialogue, choose to Keep or Remove the text formatting for the pasted content.

The HTML editor has some pasting limitations:

- Pasting images: Pasting images and text from OneNote works in Microsoft browsers. Pasting from OneNote into Chrome or Firefox works but styles and images are not included. You can still select images individually and paste them into the HTML field. Pasting images and text from Microsoft Word into any browser works as expected.
- Pasting tables: Pasting tables into Safari does not always work correctly. Pasting tables into Internet Explorer only works from Excel.

**Image field type**

Image fields enable you to add images to forms.

Role required: personalize_form

For example, you can add portraits to the user records in your system. The image type must be .gif, .jpg/.jpeg, or .png.
Image resizing is defined by the CSS. Larger images are resized to 250 pixels. For most browsers, the larger of the height and width measurements is reduced to 250 pixels and the proportion of the image is maintained. For example, an image with a size of 1508 x 663 pixels is resized to 250 x 110 pixels. Some browsers resize both the height and width measurements to 250 pixels, resulting in a square image.

You can add a new image field.

1. Open the desired form.
2. Create a new field with the Type set to Image.
   For instructions, see Add and customize a field in a table.
3. Add the new field to the form and save your customization.
   The form displays the new blank image field.
4. Click Click to add in the image field, select an image to upload, and click OK.
   The selected image is attached to the form and displayed in the image field.

**IP address field type**

The IP Address (Validated IPV4, IPV6) [ip_addr] field type stores valid IPv4 and IPv6 addresses.

**Support for IPv4 and IPv6**

Both dot-decimal and hex notation are supported for IPv4 and IPv6. For IPv6, you can use the double-colon notation to compress zeros. Familiarize yourself with IETF RFC5952 for examples and guidelines on text representation for IPv6 addresses.

The following are examples of valid IP addresses:

- **A standard IPv4 address in dot-decimal notation:**
  10.34.51.20

- **A same IPv4 address in hex notation:**
  0x0A223314 or 0A223314

  **Note:** The optional prefix 0x is supported.

- **A standard IPv6 address in dot-decimal notation:**
  1507:00d0:1002:0051:0000:0000:0000:0004
- The same IPv6 address above using the double-colon in place of zeros:
  1507:f0d0:1002:51::4

How IP addresses are stored in the database

The IP address `ip_addr` field is a Variable Character (VARCHAR) field with a length of 45 characters. The values are always stored in four-digit groupings in doc-decimal notation for both IPv4 or IPv6 addresses regardless of the notation you use when you input values in the field. For example:

- If you enter an IPv6 IP address in an using double-colons, the value in the database is actually expanded to its full IP address without compression: 1507:f0d0:1002:51::4 is saved in the database as 1507:f0d0:1002:0051:0000:0000:0000:0004
- If you enter an IPv4 address in hex notation, it is saved in the database as the standard dot-decimal notation: 0x0A223314 is saved as 10.34.51.20.

If you run a query on this field type in scripts, make sure to query on the full dot-decimal notation.

Journal field type

There are three types of journal field: journal, journal_list, and journal_input.

<table>
<thead>
<tr>
<th>Journal field types</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>journal</td>
<td>Allow and store input, and display the combined inputs below the input box. Journal fields display in the activity stream in the form and in the list view.</td>
</tr>
<tr>
<td>journal_input</td>
<td>Allow and store input, but do not display the combined inputs. Journal input fields only display with the record they are associated with, so they do not display in the activity stream on the list view.</td>
</tr>
<tr>
<td>journal_list</td>
<td>Do not allow or store input; they merely display the contents of other Journal fields upon which the journal_list field is dependent. If a journal_list field is dependent on more than one Journal field, it will chronologically interweave those fields' inputs. The journal_list field does not display content within the activity stream, but rather in a separate block.</td>
</tr>
</tbody>
</table>
The example image contains the three available journal field types. The first is a journal field, with its inputs displayed below the field. The second is a journal input field, which does not show its previous inputs. The third is Journal list field, which is configured to show the input from the journal input field above it.

**Journal fields examples on a form**

**Restricting journal entries sent in a notification**

Administrators can control the number of journal entries notifications include with the following system property.

<table>
<thead>
<tr>
<th>Property</th>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.email.journal.lines</td>
<td>Number of journal entries (Additional comments, Work notes, etc.) included in email notifications (-1 means all).</td>
<td>Specifies the number of entries from a journal field (such as Additional comments and Work notes) included in email notifications. A value of -1 includes all journal entries.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: integer&lt;br&gt;• Default value: 3&lt;br&gt;• Location: System Properties &gt; Email</td>
</tr>
</tbody>
</table>
Code for getting the contents of a journal field into an array

To put the contents of a journal field into an array so that you can iterate through each entry, you can use the code in this page.

```javascript
// gets all journal entries as a string where each entry is delimited by '
 \n'
var notes = current.work_notes.getJournalEntry(-1);

// stores each entry into an array of strings
var na = notes.split("\n\n");

for (var i = 0; i < na.length; i++)
  gs.print(na[i]);
```

Journal field script values

The `setValue()` method is not supported for journal fields. Instead, assign values in script as in the following example.

```javascript
var now_GR = new GlideRecord('incident');

// query priority 1 incidents in the state of either 'new' or 'active'.
gr.addQuery('priority', 1);
var gc = gr.addQuery('state', 1);
gc.addOrCondition('state', 2);
gr.query();

while(gr.next())
{
  // print a list of the incident numbers updated
  gs.print(gr.number);

  // add an entry to the 'work notes' journal field for each incident
  gr.work_notes = "This is a high-priority incident. Please prioritize."
  gr.update();
}
```

Render journal field entries as HTML

Journal fields can render text enclosed within code tags as HTML.

- Role required: any role that grants write access to a journal field
- System property: the glide.ui.security.allow_codetag is set to the default value of `true`

Note:

To learn more about this property, see Allow JavaScript tags in embedded HTML (instance security hardening) in Instance Security Hardening Settings.
By default, a High Security Setting escapes any HTML code you type in a journal field by replacing it with its equivalent HTML entity value. Escaping causes the system to display HTML code as text rather than forwarding it to the browser as rendering instructions.

1. Enter `[code][/code]` tags around any code you want to render as HTML.

   **Note:** A single journal entry can contain multiple code tags as long as each code tag has a beginning and ending tag.

For example, enter these lines:

**Results of entering HTML code**

<table>
<thead>
<tr>
<th>Code entered</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>[code]&lt;b&gt;This text will be bold. &lt;/b&gt;[/code]</code></td>
<td>The system renders the sentence in bold.</td>
</tr>
<tr>
<td><code>&lt;b&gt;This text will not be bold.&lt;/b&gt;</code></td>
<td>The system escapes the bold tags and renders them as text.</td>
</tr>
<tr>
<td><code>[code]&lt;script&gt;gs.info(gs.getUserDisplayName());&lt;/script&gt;[/code]</code></td>
<td>The system escapes the content of the script tag.</td>
</tr>
</tbody>
</table>

**Note:** By default, the HTML Sanitizer prevents the entry of `<script>` elements.

For more examples of HTML formatting options, see the blog post [Formatting within Journal fields using HTML & `[code]`](https://community.servicenow.com) by a ServiceNow Technical Support Engineer in the Now Community.

2. Click *Post*.

   **Note:** You cannot edit previous journal entries.

The system renders the text within code tags as HTML.

**Restrict the CODE tag in journal fields**

You can prevent journal fields from rendering HTML code by disabling support for the `[code]` tag.

Role required: admin

1. Navigate to *System Properties > UI Properties*.
2. Clear the check box for *Allow support for embedding HTML code by using the [code] tag* (the `glide.ui.security.allow_codetag` property).

   **Note:** To learn more about this property, see [Allow embedded HTML code (instance security hardening)](https://community.servicenow.com) in the Instance Security Hardening Settings.

3. Click *Save*.

**Validate HTML in journal fields**

You can prevent users from saving invalid HTML in a journal field.

Role required: admin

1. Add the property `glide.ui.allow_deep_html_validation`. For instructions, see [Add a system property](https://community.servicenow.com).
2. Set the **Value** to **true** (it is false by default).
3. Click **Save**.

Users now see a warning in the activity formatter when they enter invalid HTML code in a journal field.

![Activity](https://via.placeholder.com/150)

### Journal field display limits

Journal fields can greatly increase the size of task records because they allow users to enter very large string values. Display limits prevent the instance from loading the entire journal field into memory. Administrators have the option to:

- Set the length at which journal fields stop displaying the entire field's contents and instead only display a portion (called a preview) of the field's contents. Users can still access the field's entire contents by clicking a **Show All** button.
- Set the size of the preview text the journal field displays.
- Set the maximum number of journal entries journal fields can display.

In UI16, journal fields and the activity formatter must be in the same form section. You cannot place another field in between a journal field and the activities formatter. The Activity Stream is built to keep journal fields stacked on top of the activity formatter.

**Note:** Journal field display limits are not supported in the legacy **Comments and Worknotes** field.

---

**Set the maximum display size for journal fields**

You can set the maximum display size for journal fields by adding a system property.

Role required: admin

When a journal field exceeds the length set in this property, the instance shows a preview of the journal field instead of the field's entire contents. The preview includes a **Show All** button to display the rest of the field's contents. A separate property determines the number of characters the preview displays.

1. **Add a system property** with the following settings.

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>glide.max_journal_list_size</td>
</tr>
<tr>
<td>Description</td>
<td>Size in megabytes when a journal field should display a preview rather than the field's entire contents.</td>
</tr>
<tr>
<td>Type</td>
<td>Integer</td>
</tr>
<tr>
<td>Value</td>
<td>10</td>
</tr>
</tbody>
</table>

2. Click **Submit**.
Set the journal preview size
When a journal field exceeds the size of the `glide.max_journal_list_size` property, the instance displays a preview rather than the field's entire contents.

Role required: admin

To specify the amount of text to display as a preview, set the following system property. Users can click the **Show All** button to see the rest of the field's contents.

- Add a system property with the following settings. For instructions, see Add a system property.

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>glide.shortened_journal_length</td>
</tr>
<tr>
<td>Description</td>
<td>Number of characters to display as a preview of journal fields.</td>
</tr>
<tr>
<td>Type</td>
<td>Integer</td>
</tr>
<tr>
<td>Value</td>
<td>512000</td>
</tr>
</tbody>
</table>

Set the maximum number of journal entries
To set the maximum number of entries the system shows in the activity formatter, edit the following system property. The activity formatter displays the entries starting with the most recent entry up to the maximum number.

Role required: admin

1. Enter `sys_properties.list` in the navigation filter.
2. Search for the property `glide.history.max_entries`.
3. Edit the **Value** of the property.

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>glide.history.max_entries</td>
</tr>
<tr>
<td>Description</td>
<td>Maximum number of entries the system shows in the activity formatter. The default is 250.</td>
</tr>
<tr>
<td>Type</td>
<td>Integer</td>
</tr>
<tr>
<td>Value</td>
<td>250</td>
</tr>
</tbody>
</table>

4. Click **Update**.

Enable the text field character counter
By default, multi-line text fields have a 4000 character limit. To help users see how many characters remain before they reach the limit, you can enable the `glide.ui.textarea.character_counter` property.

Role required: admin

This property adds a counter under text fields, such as the **Additional Comments** and **Work notes** fields. The counter is dynamically updated as users enter text.

1. Navigate to **System Properties > UI Properties**.
2. Select the check box next to **Character counter for textarea (journal and multi line text fields)**.
3. Click **Save**.

---

**Disable or enable spell checking on a journal field**

Spell checking is turned on by default on most input fields, except for single-line input fields. The spell checker highlights misspelled words.

Role required: personalize_dictionary

To enable the spell checking dictionary, install the appropriate language plugin. Localization plugins have the same name format, such as I18: German Translations.

The dictionaries available for spell checking include the following languages:

- Brazilian Portuguese
- Czech
- Dutch
- English US
- English UK
- Estonian
- Finnish
- French
- German
- Hebrew
- Hungarian
- Italian
- Polish
- Portuguese
- Russian
- Spanish
- Thai

**Note:** The words in the dictionary are part of the language plugin. You cannot add, remove, or modify the dictionary.

You can select a dictionary to use for a language that does not have a spell checker dictionary by navigating to **System Properties > System Localization**.
1. Navigate to **System Definition > Dictionary**.
2. Filter the list to view **journal** type fields and select a field to spell check.
   An example is the **comments** field in the Task table. This applies spell checking in the specified language to the multi-line **Comments** text box for incidents, problems, and changes.
3. Click the table name to open the Dictionary form.
4. Configure the form and add the **Spell check** check box.
5. Clear the check box to disable spell checking in every **Comments** field on the Task table.

**Name-value pairs field type**

You can access the values stored in a name-value pairs field in scripts using the name.

**Sample script**

The following example demonstrates how to add mappings to a name-value pairs field, and how to query existing values using the name.

```javascript
// Script example demonstrating setting and getting values
var now_GR = new GlideRecord('u_nv_table');
gr.initialize();

gr.nv_field.name1 = "value1"; //add a name-value Pair mapping with the name "name1" and value "value1"
gr.nv_field.name2 = "value2"; //add another name-value Pair mapping with the name "name2" and value "value2"

// Access by dot notation
gs.print("name1 = " + gr.nv_field.name1); // Expected output: name1 = value1

// Iterate over each property and print name and value
for(var name in gr.nv_field) {
    gs.print(name + " = " + gr.nv_field[name]);
}

gs.print(gr.nv_field); // Expected output:
{"name1":"value1","name2":"value2"}
```
Percent complete field type

Administrators can create percent complete fields, which accept decimal input and appear as progress bars when displayed in lists.

For example, use a percent complete field to set the completion percentage for a task or project in a form and then see that percentage displayed as a progress bar in a list.

Administrators can also configure views that compare actual progress with a target value to determine if goals are being met and then apply color to provide visual alerts where progress does not meet expectations.

Form view of a percent complete field

List view of a percent complete field

Target threshold colors attribute

If the target_field attribute is configured, a second attribute called target_threshold_colors enables an administrator to define additional parameters.

The parameters are:

- Different thresholds at which the colored bar should change color
- A specific color for each threshold

The format of this attribute's value is number1:color1;number2:color2 and so on. Use this attribute to apply warning colors to completion percentages that are lower than target percentages. These values are defined as the percentage of target accomplished. For example, a value of 0:red;50:yellow;90:green displays a red bar if the progress to target percentage is between 0-49. If the percent of target is between 50 and 89, the color is yellow. Percent of target 90 and above displays in green. Completion percentages that exceed target percentages also display in green. Order the color attributes from the smallest percentage to the largest.

If you do not specify a target_field, then a target of 100 is used, allowing you to use the color thresholds with a single field value.

target_field=percent_complete_target,target_threshold_colors=0:tomato;50:khaki;90:lightgreen

The following table lists examples of percent of target calculation using the colors defined above.

Target threshold colors attribute

<table>
<thead>
<tr>
<th>Target percent</th>
<th>Percent field value</th>
<th>Percent of target calculation</th>
<th>Color</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>40</td>
<td>40%</td>
<td>tomato</td>
</tr>
</tbody>
</table>
Percent complete color example

Add a target field attribute

Add an optional attribute (target_field) to a percent complete field to compare the actual completion percentage of a task or project with a target percentage in a different decimal field that specifies where the task should be at this point.

Role required: personalize_dictionary

If a target field is not specified, the target of 100 is assumed.

1. Right-click the % Complete field in a form.
2. Select Configure Dictionary from the pop-up menu.
3. In the Dictionary Entry form, add the following attribute:
   
   target_field=percent_complete_target

4. Update the dictionary record.

In the list, a gray bar appears behind the colored bar to indicate the target value. The gray target bar appears only if you defined a target field.
Phone number field type

The E.164 phone number standard ensures that all necessary information for a phone number is included and properly formatted to successfully route an international call over a territory's public telephone network.

When a user enters a phone number, it is received and stored as a string of numbers. An E.164 phone number field automatically formats and validates the numbers so that they are E.164-compliant when displayed as local and international numbers. The E.164 phone number field type does not replace the phone field type.

An E.164 phone number field displays:

- [Optional] A choice list for the phone number territory.
- [Always] An input box for entering phone numbers.
- [By Default] A red underline when a phone number does not match the format for the selected phone territory and cannot be saved.
- [Optional] A green underline when a phone number does not match the format for the selected phone territory but can be saved with Other / Unknown as the territory.

Territories assigned

Territories are assigned to locations, and are not assigned directly to users.

A user's territory, and so the user's E.164-compliant phone functionality, is based on the user's location. For example, if a user has a location of SHS quadra 5, Bloco E., Brasilia defined in the User [sys_user] table, the parent record for Brazil in the location table defines the phone territory. The phone territory may be assigned at any level of the location hierarchy, which is searched going up to the next parent until the territory is found or no parents remain.

Dependent fields

In the dictionary, you can specify a dependent field in the User or Location field, which displays the appropriate territory in the selector choice list when a user enters a phone number.

In the dictionary, you can specify a dependent field in the User or Location field, which displays the appropriate territory in the selector choice list when a user enters a phone number. For example, if you enter caller_id in the dependent field in the Incident table, the appropriate territory is added to the territory selector choice list when a user enters caller information.

E.164 phone number field configuration

Administrators can use the phone number system properties and dictionary attributes to do certain things.

The system properties apply the configuration option to all phone number fields that do not have a comparable dictionary attribute. The dictionary attributes apply the configuration only to the phone number field it is added to. Since dictionary attributes take precedence over system properties, administrators can set a global configuration with a property and then apply exceptions on a field-by-field basis.

Requiring territory format validation

By default, phone number fields require that a phone number match the display format of the selected territory.

By default, phone number fields require that a phone number match the display format of the selected territory. If a phone number does not match this format, the input box displays a red line underneath the phone number and users are prevented from saving it.
Setting the `glide.phone_number_e164.strict` system property to `false` or adding the `pn.strict` dictionary attribute allows the phone number input box to display a green line underneath numbers that do not match the territory format listed for the selected territory. In this case, a user can save a phone number in an invalid format, but the field continues to display a warning until the phone number matches the format required by the territory. You can use the `Other / Unknown` territory to store otherwise invalid phone numbers.

**Warning:** Switching from optional territory format validation to required territory format validation may result in some phone numbers failing validation altogether. In such cases, the E.164 phone number field displays an error message.

**Requiring entry of international format**

By default, users can enter phone numbers in their territory's local format and do not have to format the number for international dialing.

The phone number field automatically formats local phone numbers into E.164-compliant international phone numbers when the user finishes editing the field. As long as the phone number entered matches the territory's format for a local number, users can save the phone number.

Changing the `glide.phone_number_e164.allow_national_entry` system property or adding the `pn.allow_national_entry` dictionary attribute requires users to enter a phone number in the territory's international format, which starts with the plus (+) character. Users cannot save a locally formatted phone number, and the phone number input box displays a red line underneath phone numbers without the proper international formatting.

**Configure the display of the local format**

By default, an E.164 phone number field always displays phone numbers in an international format.
Change the E.164 phone number to use the local format in certain circumstances by adding the following system property:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| glide.phone_number_e164.display_national | • **Type**: string  
• **Default value**: false  
• **Other possible values**:  
  • **true or form**: displays phone numbers in a local format on forms, but displays an international format on lists.  
  • **all**: always displays phone numbers in a local format.  
  • **user**: only displays phone numbers in a local format when the phone number matches the local setting of the current user.  
  • **false**: does not display phone numbers in local format. |

Select one of the possible values to determine how the system handles the E.164 phone number.

You can also add the following dictionary attribute to a specific field to override the system property:

<table>
<thead>
<tr>
<th>Dictionary attribute</th>
<th>Description</th>
</tr>
</thead>
</table>
| pn_display_national  | Overrides the glide.phone_number_e164.display_national property setting for how an E.164 phone number field displays phone numbers. Available values are identical to those described for the glide.phone_number_e164.display_national property.  
  • **Type**: string  
  • **Default value**: false  
  • **Example**: pn_display_national=all |

Configure the phone territory selector choice list
By default, an E.164 phone number field always displays the phone territory associated with the phone number.

Changing the system property or adding the dictionary attribute hides the territory selector choice list. If the territory selector choice list is hidden, users can only enter a local or national number.

Phone e164 hide selector

Add the following system property to show or hide the territory selector choice list.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| glide.phone_number_e164.display_territory_selector | Determines whether to display the territory selector choice list. Hiding the territory selector choice list restricts users to entering only local or national phone numbers.  
  • **Type**: true | false  
  • **Default value**: true |
You can also add the following dictionary attribute to a specific field to override the system property:

<table>
<thead>
<tr>
<th>Dictionary attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pn_display_territory_selector</td>
<td>Overrides the glide.phone_number_e164.display_territory_selector property setting that determines whether to display the territory selector choice list. Available values are identical to those described above for the glide.phone_number_e164.display_territory_selector property.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: true</td>
</tr>
<tr>
<td></td>
<td>• Example: pn_display_territory_selector=false</td>
</tr>
</tbody>
</table>

Configure the display of territory labels
A property controls how territory labels are displayed.

You can display territory labels to the right of the number in an E.164 phone number field by setting the system property or adding the dictionary attribute. This is useful if the territory selector choice list is turned off and you want the user to see the territory for the entered phone number.

Enabling territory labels also displays the phone territory in lists.

Add the following system property to display the territory label to the right of the number in an E.164 phone number.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.phone_number_e164.display_territory_text</td>
<td>Determines when an E.164 phone number field displays a territory label.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: read-only</td>
</tr>
<tr>
<td></td>
<td>• Other possible values:</td>
</tr>
<tr>
<td></td>
<td>• all: always displays the territory label.</td>
</tr>
<tr>
<td></td>
<td>• national: displays the territory label only if the phone number is in local format.</td>
</tr>
<tr>
<td></td>
<td>• read-only: displays the territory label in read-only mode, regardless of whether the number is in local or international format.</td>
</tr>
<tr>
<td></td>
<td>• read-only-national: displays the territory label in read-only mode only if the number is in local format.</td>
</tr>
<tr>
<td></td>
<td>• list: displays the territory label in a list.</td>
</tr>
<tr>
<td></td>
<td>• list-national: displays the territory label in a list if the number is in national format.</td>
</tr>
<tr>
<td></td>
<td>• none: does not display the territory label.</td>
</tr>
</tbody>
</table>

You can also add the following dictionary attribute to a specific field to override the system property:
Configure the international direct dialing prefixes

A property is available to control the display of prefixes.

You can enable the display of the international direct dialing prefix, which appears between the territory selector choice list and the input box for an E.164 phone number field on forms, by setting the system property or adding the dictionary attribute.

![E164 phone display idd](image)

Add the following system property to display the international direct dialing prefix.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.phone_number_e164.display_users_idd</td>
<td>Determines whether to display the international direct dialing prefix between the territory selector choice list and the input box on forms.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: false</td>
</tr>
</tbody>
</table>

You can also add the following dictionary attribute to a specific field to override the system property:

<table>
<thead>
<tr>
<th>Dictionary attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pn_display_users_idd</td>
<td>Overrides the glide.phone_number_e164.display_users_idd property that determines whether to display the international direct dialing prefix between the territory selector choice list and the input box on forms. Available values are identical to those described above for the glide.phone_number_e164.display_users_idd property.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: false</td>
</tr>
<tr>
<td></td>
<td>• Example:pn_display_users_idd=false</td>
</tr>
</tbody>
</table>
E.164 phone number field system properties
Several properties are available to configure E.164 phone number fields.

Note: To open the System Properties [sys_properties] table, enter `sys_properties.list` in the navigation filter.

e.164 phone number field system properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.phone_number_e164.strict</td>
<td>Determines whether all phone number fields must match the display format for the selected territory. When the value is <code>true</code>, the phone number input box displays a red line underneath phone numbers that do not match the format for the selected territory. Users cannot save the phone number. When the value is <code>false</code>, the phone number input box displays a green line underneath phone numbers that do not match the format for the selected territory. Users can save the phone number. The territory selector choice list offers the option to select an Other / Unknown territory format.</td>
</tr>
<tr>
<td>Type: true</td>
<td>false</td>
</tr>
<tr>
<td>Default value: true</td>
<td></td>
</tr>
<tr>
<td>Location: Add to the System Properties [sys_properties] table.</td>
<td></td>
</tr>
<tr>
<td>glide.phone_number_e164.allow_national_entry</td>
<td>Determines whether users can enter phone numbers in the local format or whether they must enter phone numbers in international format. When <code>true</code>, users can enter phone numbers in the local format for the selected territory. When <code>false</code>, users must enter phone numbers in the international format for the selected territory.</td>
</tr>
<tr>
<td>Type: true</td>
<td>false</td>
</tr>
<tr>
<td>Default value: true</td>
<td></td>
</tr>
<tr>
<td>Location: Add to the System Properties [sys_properties] table.</td>
<td></td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>glide.phone_number_e164.display_national</td>
<td>Determines whether to display E.164 phone numbers in local format.</td>
</tr>
</tbody>
</table>
| | • **Type**: string  
| | • **Default value**: false  
| | • **Other possible values**:  
| | • **true or form**: Displays phone numbers in a local format on forms, but displays an international format on lists.  
| | • **all**: Always displays phone numbers in a local format.  
| | • **user**: Only displays phone numbers in a local format when the phone number matches the local setting of the current user. The local setting of the current user is determined by the country code and the language associated with a specific user record.  
| | • **false**: Does not display phone numbers in local format.  
| | • **Location**: Add to the System Properties [sys_properties] table. |

| glide.phone_number_e164.display_territory_selector | Determines whether to display the territory selector choice list. Hiding the territory selector choice list restricts users to entering only local or national phone numbers. |
| | • **Type**: true | false  
| | • **Default value**: true  
<p>| | • <strong>Location</strong>: Add to the System Properties [sys_properties] table. |</p>
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| glide.phone_number_e164.display_territory_text | Determines when an E.164 phone number field displays a territory label.  
  - **Type**: string  
  - **Default value**: read-only  
  - **Other possible values**:  
    - **all**: always displays the territory label.  
    - **national**: displays the territory label only if the phone number is in local format.  
    - **read-only**: displays the territory label in read-only mode, regardless of whether the number is in local or international format.  
    - **read-only-national**: displays the territory label in read-only mode only if the number is in local format.  
    - **list**: displays the territory label in a list.  
    - **list-national**: displays the territory label in a list if the number is in national format.  
    - **none**: does not display the territory label.  
  - **Location**: Add to the System Properties [sys_properties] table. |
| glide.phone_number_e164.display_users_idd | Determines whether to display the international direct dialing prefix between the territory selector choice list and the input box on forms.  
  - **Type**: true | false  
  - **Default value**: false  
  - **Location**: Add to the System Properties [sys_properties] table. |

**E.164 phone number field dictionary attributes**  
You can override the global system property with certain dictionary attributes.

**e.164 phone number field dictionary attributes**

<table>
<thead>
<tr>
<th>Dictionary attribute</th>
<th>Description</th>
</tr>
</thead>
</table>
| pn_strict | Overrides the `glide.phone_number_e164.strict` property setting that requires all phone number entries match the format for the selected territory. Available values are identical to those described for the `glide.phone_number_e164.strict` property.  
  - **Type**: true | false  
  - **Default value**: true  
  - **Example**: `pn_strict=false` |
<table>
<thead>
<tr>
<th>Dictionary attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pn_allow_national_entry</td>
<td>Overrides the <code>glide.phone_number_e164.allow_national_entry</code> property setting that determines whether users can enter phone numbers in the local format or whether they must enter phone numbers in international format. Available values are identical to those described for the <code>glide.phone_number_e164.allow_national_entry</code> property.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: true</td>
</tr>
<tr>
<td></td>
<td>• Example: pn_allow_national_entry=false</td>
</tr>
<tr>
<td>pn_display_national</td>
<td>Overrides the <code>glide.phone_number_e164.display_national</code> property setting for how an E.164 phone number field displays phone numbers. Available values are identical to those described for the <code>glide.phone_number_e164.display_national</code> property.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: false</td>
</tr>
<tr>
<td></td>
<td>• Example: pn_display_national=all</td>
</tr>
<tr>
<td>pn_display_territory_selector</td>
<td>Overrides the <code>glide.phone_number_e164.display_territory_selector</code> property setting that determines whether to display the territory selector choice list. Available values are identical to those described for the <code>glide.phone_number_e164.display_territory_selector</code> property.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: true</td>
</tr>
<tr>
<td></td>
<td>• Example: pn_display_territory_selector=false</td>
</tr>
<tr>
<td>pn_display_territory_text</td>
<td>Overrides the <code>glide.phone_number_e164.display_territory_text</code> property that defines when a phone number field displays a territory label. Available values are identical to those described for the <code>glide.phone_number_e164.display_territory_text</code> property.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: read-only</td>
</tr>
<tr>
<td></td>
<td>• Example: pn_display_territory_text=all</td>
</tr>
</tbody>
</table>
Configure a territory phone display rule

The string of numbers that make up a phone number is automatically validated and formatted for a specific territory by applying a series of regular expressions.

Role required: admin

The number is first validated against the phone validations that have been defined for the territory, and in the order specified by the Order field. To be valid, the number must match the regular expression defined in the Condition field for at least one phone validation.

After a number has been validated, the Condition expression for each format defined for the territory is applied to the number in the order determined by the Order fields. The Pattern and Format regular expressions are applied to produce a phone number that is formatted correctly for the territory.

The Sys Phone Territory screen allows administrators to edit the display rules for a given territory. Administrators may want to modify the Active, Display, or Order fields. To edit the display rules for a territory:

2. Click a territory Name.
3. Edit the fields, as appropriate (see table).
4. Click Update.

<table>
<thead>
<tr>
<th>Dictionary attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pn_display_users_idd</td>
<td>Overrides the glide.phone_number_e164.display_users_idd property that determines whether to display the international direct dialing prefix between the territory selector choice list and the input box on forms. Available values are identical to those described for the glide.phone_number_e164.display_users_idd property.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: false</td>
</tr>
<tr>
<td></td>
<td>• Example: pn_display_users_idd=false</td>
</tr>
</tbody>
</table>
## Territory phone display rules

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The unique name of the territory.</td>
</tr>
<tr>
<td>Country calling code</td>
<td>The country code for dialing numbers from outside the territory.</td>
</tr>
<tr>
<td>International direct dial</td>
<td>The prefix for calling internationally from the territory, such as 00 or 001.</td>
</tr>
<tr>
<td>STD</td>
<td>The subscriber trunk dialing code, also known as the direct distance dialing code, which is a sequence of numbers before the telephone number that indicate whether the call is to be routed outside of the local calling area.</td>
</tr>
<tr>
<td>International prefix</td>
<td>The prefix required to dial an international call, such as a plus sign (+).</td>
</tr>
<tr>
<td>National prefix</td>
<td>The prefix required to dial a local call.</td>
</tr>
<tr>
<td>Active</td>
<td>An indicator for whether the territory phone definition is active. If deactivated, this territory unavailable to users.</td>
</tr>
<tr>
<td>Trunk dialing code optional</td>
<td>An indicator for whether the STD code is optional.</td>
</tr>
<tr>
<td>STD follows country</td>
<td>An indicator for whether the STD code should be displayed to the right of the country calling code.</td>
</tr>
<tr>
<td>Display</td>
<td>An indicator for whether to display the territory in the choice list. Clearing this check box removes the territory from the choice list. If an international number is entered for a territory that is not displayed in the territory selector choice list, that territory is temporarily added to the selector choice list for that field only. For example, if the United Kingdom Display field is not selected, the United Kingdom does not appear in the territory selector choice list. However, if the user enters an international number beginning with +44, the United Kingdom is added to the list and the number is formatted and validated accordingly.</td>
</tr>
<tr>
<td>Order</td>
<td>The order in which a territory appears in a choice list. Territories are sorted numerically by the number assigned here. If more than one territory is assigned the same number, they are subsorted alphabetically. All territories are assigned a default value of 100. To display a territory at the top of the list, assign a value that is less than 100. To display a territory at the end of the list, assign a value that is greater than 100. For example, if a territory is assigned an order of 500, it is displayed at the end of the list, and if more than one territory is assigned an order of 500, they are listed alphabetically at the end of the list.</td>
</tr>
</tbody>
</table>
Phone validations

Phone validations are already configured for all territories and are automatically applied to the phone number to ensure that the number is valid for the territory.

E164 phone validations

Phone formats

Phone formats are already configured for all territories and are automatically applied to the phone number to ensure that the number is valid for the territory.

E164 phone formats

Reference field type

A reference field stores a reference to a field on another table. For example, the Caller field on the Incident table is a reference to the User [sys_user] table.

When you define a reference field, the system creates a relationship between the two tables. Adding a reference field to a form makes the other fields in the referenced table available to the form.
Administrators can create new reference fields and configure several options for reference fields.

**Reference field options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display values</td>
<td>Each reference field stores a sys_id for each referenced record in the database, but the sys_id is not shown. The reference field shows the specified display value.</td>
</tr>
<tr>
<td>Decorations</td>
<td>A reference decoration is an icon that appears next to a reference field.</td>
</tr>
<tr>
<td>Reference styles</td>
<td>Reference styles are specialized field styles that control the appearance of reference fields.</td>
</tr>
<tr>
<td>Reference qualifiers</td>
<td>Reference qualifiers restrict the records that are available for reference fields.</td>
</tr>
<tr>
<td>Cascade delete rules</td>
<td>Cascade delete rules specify what should happen to records that reference a record that is deleted.</td>
</tr>
<tr>
<td>Auto-complete</td>
<td>By default, a reference field auto-completes as the user types in the field. Administrators can configure auto-complete settings.</td>
</tr>
<tr>
<td>Reference key</td>
<td>A reference key saves a field other than sys_id as the unique identifier for a reference field.</td>
</tr>
<tr>
<td>Enable dynamic creation</td>
<td>When dynamic creation is enabled, entering a nonexistent value in a reference field creates a new record on the referenced table instead of returning an error.</td>
</tr>
</tbody>
</table>

**Add a reference field**

Add reference fields to a table using the same method as for any other field.

Role required: personalize_form

The related table also appears in the Available Tables list for future form customizations.

1. Open the desired form.
2. Right-click the header and select **Configure > Form Layout**.
3. Use **dot-walking** to locate and select the field in the referenced table that you want to add.
   It appears as **Table name.Field**. For example, the caller's email address appears as **Caller.Email**.
4. Click **Save**.

**Enable dynamic creation for reference fields**

When dynamic creation is enabled, entering a nonexistent value in a reference field creates a new record on the referenced table instead of returning an error.

Role required: personalize_dictionary

By default, a user must enter a value in a reference field that matches an existing record in the table that the reference field refers to. For example, the **Caller** field in an Incident must have a value that is an existing user. You can enable
dynamic creation to create a new record on the referenced table when a user enter a nonexistent value in a reference field instead of returning an error.

1. Right-click the field label in the form and select **Configure Dictionary**.
2. Populate the following fields (you may need to configure the Dictionary form):
   
   - **dynamic_creation**: Select the check box.
   - **dynamic_creation_script**: Enter a script that dynamically creates the record.

3. Click **Update**.

Examples:

You could use the following `dynamic_creation_script` to create a record on the referenced table.

```javascript
current.name = value;
current.insert();
```

**Note**: The parent object can be used to access anything from the parent record.

You could create a script include named `MyUserReferenceCreator` with the following contents:

```javascript
var MyUserReferenceCreator = Class.create();
MyUserReferenceCreator.prototype = {
   initialize: function() {
   },
   create: function(current, value) {
      current.name=value;
      return current.insert();
   },
   type: 'MyUserReferenceCreator'
}
```

When the script include is created, the following `dynamic_creation_script` generates a new location for an invalid reference field value:

```javascript
new MyUserReferenceCreator().create(current, value);
```

**Configure cascade delete rules**

When a record is deleted, there are different options for how the deletion will affect records that reference the deleted record. You can configure what happens to records that reference a record when that record is deleted.

Role required: personalize_dictionary

For example, if you delete a user record that is referenced in the **Caller ID** field on several incident records, you can configure what happens to those incident records. By default, the references are cleared, so the incident records are maintained with an empty **Caller ID** field.

1. Navigate to a reference field on a form.
2. Right-click the field label and select **Configure Dictionary**.
3. Under **Related Links**, click **Advanced view**.
5. In the **Reference cascade rule** field, select one of the following options.

   ![Note: The option for this field have no effect for tables with m2m relationships, meaning that in this example, if the tables have an m2m relationship, the user record is deleted.]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear or -- None --</td>
<td>Deleting a record clears references (default option).</td>
</tr>
<tr>
<td>Delete or Cascade</td>
<td>Deleting a record also deletes all referencing records. For example, when a user record is deleted, any incidents assigned to the user are also deleted. <strong>CAUTION:</strong> Use this method with caution.</td>
</tr>
<tr>
<td>Restrict</td>
<td>Deleting a record is restricted unless there are no references to the record. For example, prevent the user record from being deleted if any incident includes a reference to the user.</td>
</tr>
<tr>
<td>None</td>
<td>Deleting a record does not change records that reference the record.</td>
</tr>
</tbody>
</table>

6. Click **Update**.

**Define the reference key**

By default, reference fields store the sys_id of the record in the database.

Role required: personalize_dictionary

By defining a reference key, you can identify a field other than sys_id to use as the unique identifier for the reference field. The value of the reference key field, instead of the sys_id, is stored in the database for that reference field.

1. Navigate to **System Definition > Dictionary**.
2. Open the field record (for example, **resolved_by** on the Incident table).
3. In the **Reference key** field, enter a field name on the referenced table (for example, email on the sys_user table). 
   
   ![Note: Always choose a field from the referenced table that is both required and unique.]

4. Click **Update**.
Display a reference field as a choice list
You can display a reference field as a choice list instead of opening a lookup window.

Role required: personalize_dictionary

1. In the form, right-click the label for the reference field and select Configure Dictionary.
2. In the Choice List Specification section, select one of the following options in the Choice field.
   - Dropdown with --None--
   - Dropdown without --None--
3. Right-click the form header and click Save.
5. In the Attributes field, add the following attribute, separated from other attributes by a comma.
   

ref_auto_completer=AJAXReferenceChoice

6. Click Update.
The form reopens, with the reference field as a choice list.

Note:
The glide.ui.max_ref_dropdown system property determines whether a reference field is displayed as a choice list or a reference icon. When the number of available choices exceeds the value of this
property, a reference icon displays instead of a choice list. The default value of this property is 25. This property affects the entire instance, however you can override this property on an individual field by using the `max_ref_dropdown` dictionary attribute. Modifying dictionary attributes requires the personalize_dictionary role.

The `glide.xmlhttp.max_choices` system property determines how many choices display on a choice list. This property has a value of 15 by default, however, when the property is not present on the instance, the instance uses a hard coded value of 10.

### Display values

Reference fields store a sys_id for each referenced record in the database, but the sys_id is not shown.

The reference field shows the display value. For example, an incident's **Assigned to** field stores the sys_id of a particular user, but actually displays the user's name. The following example shows how **Charlie Witherspoon**, which is the display value of a user record, is shown in the **Assigned to** field.

```
<xml>
    <incident>
        <active>true</active>
        <activity_due/>
        <approval/>
        <approval_history/>
        <approval_set/>
        <assigned_to display_value="Charlie Witherspoon">46b87022a9fe198101a78787e40d7547</assigned_to>
    </incident>
</xml>
```

### Display value xml

<table>
<thead>
<tr>
<th>Reference field</th>
<th>Value stored in database</th>
<th>Display value field of source table</th>
<th>Value displayed in UI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigned to [task.assigned_to]</td>
<td>46b87022a9fe198101a78787e40d7547</td>
<td><code>[sys_user.name]</code></td>
<td>Charlie Witherspoon</td>
</tr>
</tbody>
</table>

Reference fields show display values in:

- Lists
- Forms
- Reports
- Auto-complete suggestions
- Slushbuckets

**Select a field as the table display value**

Only one field can be defined as the display value for a table.

Role required: personalize_dictionary
When you set the **Display** value to **true**, a business rule sets the **Display** value to **false** for all other fields on the table. In previous versions, you must manually ensure that no other fields on the table have a value of **true** in the **Display** column.

**Note:** Extended tables inherit the display value of the parent table. Setting a separate display value for the extended table overrides the parent table’s display value.

1. Navigate to **System Definition > Dictionary**.
2. Filter on `[Table] [is] <name of the referenced table>`.
3. Locate the desired field and set **Display** to **true**.

For best results, choose a field that is required and unique in each record as the display value field.

Reference fields look for the display value in the following order:

a. A field with display=**true** in the system dictionary on the lowest sub-table for extended tables.

b. A field with display=**true** in the system dictionary on the parent table.

c. A field named **name** or **u_name**.

d. The **Created on** field of the referenced record.

**Decorations**

Reference decorations are icons which appear next to the reference field.

The reference lookup is always visible and is used to select a record to reference. Other reference decorations appear when a record is selected.

**Reference lookup**

On forms, the reference lookup icon (🔍) appears by editable reference fields. Clicking the reference lookup icon displays a list of records on the referenced table.

When List v3 is enabled, the list appears in a popover. Otherwise, the list appears in a pop-up window.
Reference lookup list popover
UI15 reference lookup list pop-up

Tree picker lookup

The reference lookup can be rendered in the tree picker format by modifying the dictionary and adding the attribute `tree_picker`.

You cannot customize the label names used in the tree picker. The label names are taken from the values in the table.
Reference field icon

On forms, the reference icon (i) appears by populated reference fields. Clicking the icon opens a read-only preview of the referenced record.
The preview remains open until you click somewhere else on the form.

Click **Open Record** to navigate to the referenced record.

**Note:** When using a reference icon in Service Portal, a form opens using the default view of the form rather than a popup view. Write permissions to this form are the same as opening the form in the default view in the standard UI.

Configure the reference icon view of fields

Use a table's sys_popup form view to configure the fields in the pop-up form that appear when pointing to a reference icon. If the table has no sys_popup view, the pop-up uses the default view.

Role required: personalize_form

The pop-up form displays in the top form section only.

1. To configure a reference field popup form for a table using the default sys_popup view, navigate to the following URL format, substituting the instance name and table name:

   `<your instance name>.service-now.com/<table name>.do?sysparm_view=sys_popup`

   **Note:** This URL format only shows a table and default sys_popup view. It does not work for records that use a different view.

   An example of an instance for Acme, the sys_user table, and the sys_popup default view:

   `acme.service-now.com/sys_user.do?sysparm_view=sys_popup`

2. Optional: To configure a reference field popup form for a table using a non-default sys_popup view, navigate to the following URL format, substituting the instance name, table name, and name of view:

   `<your instance name>.service-now.com/<table name>.do?sysparm_view=sys_popup,<name_of_view>`

   An example of an instance for Acme, the sys_user table, and the sys_popup ESS view:

   `acme.service-now.com/sys_user.do?sysparm_view=sys_popup,ess`

3. Configure the form to add or remove fields as appropriate.

Configure pop-ups on read-only fields

Reference pop-ups and click-throughs are hidden by default when a client script, UI policy, variable, or ACL makes the field read-only. The ability to see or click through to the target record does not depend on whether the reference field is writable. You can change the read-only setting.

Role required: admin

1. Navigate to **System Properties > UI Properties**.

2. Change the value of the **Enable click-through of a reference field when the reference field is read-only.** (*glide.ui.reference.readonly.clickthrough*) property.

   If set to true, the pop-up appears for read-only fields and for variables.

   If this system value is set to **false**, you can override the setting for a specific read-only reference field. Configure the dictionary entry and add the **readonly_clickthrough=true** attribute.
Configure the related incidents icon
You can configure an icon to appear beside a reference field in a form, such as the Caller field, to display related incidents.

Role required: admin

The show related incidents icon

displays other incidents related to the referenced record.

1. In the form, right-click the label for the reference field and select Configure Dictionary.
2. Add the ref_contributions=user_show_incidents dictionary attribute in the Attributes field.
3. Click Update.
   The form reopens and the related incidents icon appears beside the field on the right.

Configure the show workflow icon
You can configure an icon to appear beside a workflow field to display the related workflow in the Workflow Editor.

Role required: admin
The show workflow icon (⚠️) opens the workflow in the Workflow Editor.

1. In the form, right-click the label for the workflow field and select Configure > Configure Dictionary.
2. Add the ref_contributions=show_workflow dictionary attribute in the Attributes field.
3. Click Update.
   The form reopens and the show workflow icon appears beside the field on the right.

Reference qualifiers

Use reference qualifiers to create filters that restrict the data that is returned for a reference field.

A reference field stores a link (reference) to a field on another table, making the records/fields in the referenced table available to the form containing the reference field.

For example, the Assigned to field on the Incident table is a reference to the User [sys_user] table. By default, all values for the field that is being referenced appear in the reference lookup and can be directly accessed through the reference field (type ahead). Expanding on the prior example, if a reference qualifier is not defined, all users in the User table appear in the reference lookup. Including those users that are inactive. Sometimes, this might be the desired functionality. In other cases however, only a subset of the available values may be desired. In this case, create a reference qualifier to filter the available data so that only the desired values are returned and made available to the form. Such as only the active users or users that have a specific role. Reference qualifiers are robust and can consist of simple AND/OR conditions, inline JaveScript, or complex script include.

You can modify the reference qualifier for a table, and any table based on that table (parent or extended), by defining a reference qualifier through the Dictionary Entry form. You can also modify the reference qualifier only on an extended table and its children (not the parent table), through a dictionary override. You can only define a single reference qualifier per field, per form/table. Reference qualifiers are not applicable to condition builders. For information on using filtering in condition builders, see Create a dynamic filter option.

Note: Creating reference qualifiers requires knowledge of the underlying ServiceNow data model (tables and fields) and knowledge of the ServiceNow API and scripting.

You can define a reference qualifier using one of the following methods.

Simple reference qualifier

Simple reference qualifiers use AND/OR statements (conditions) to create simple filters. Use simple reference qualifiers when filtering on conditions such as whether a company is active, a user has a specific role, and/or a caller is in a specific time zone. Simple reference qualifiers can have a maximum of 13 reference qualifier conditions. For additional information on how to use condition builders, see Condition builder.
Dynamic reference qualifiers

Dynamic reference qualifiers enable you to use a dynamic filter option to run a query against a reference field to filter the returned data set. Dynamic filter options are stored filters that can contain encoded query strings, JavaScript, or script includes, and can be used in multiple dynamic reference qualifiers. Changes made to a dynamic filter option automatically apply to all reference qualifiers that use the same dynamic filter option. Use this type of reference qualifier when you want to use the same filter on multiple forms or to provide filter functionality to "non-code savvy" implementers.

The base instance provides several OOB dynamic filter options. If a dynamic filter option that meets your needs does not exist, you can create a new dynamic filter option that is specific to your requirements. An example of an OOB dynamic filter option is the reference qualifier on the Model ID field on a configuration item form, such as the Computer form. The reference qualifier calls the CI Model Qualifier dynamic filter option, which in turn calls the ModelAndCategoryFilters script include. This script include filters the data set based on the class of the CI. The only options for the model ID are options that belong to the same class as the current CI. For example, only CIs that belong to the Computer class are available in the Model ID field on the Computer form.

To locate the available dynamic filter options, navigate to System Definition # Dynamic Filter Options. In the right-corner of the Dynamic Filter Options list, click the filter icon and create the filter condition Available for ref qual is true. All dynamic filter options that can be used in dynamic reference qualifiers appear.
Dynamic reference qualifier example

Advanced reference qualifier

Advanced reference qualifiers enable you to define an inline encrypted query string or JavaScript (actual code or the name of an existing script include or business rule) filter directly in the Reference quali field of the reference qualifier. Similar to the other reference qualifier types, when the form loads, the filter is executed, and only the records that match the filter appear in the reference field. Use this type of reference qualifier for implementations that only require a simple, unique filter, that cannot be handled by a simple reference qualifier, and is not used across multiple reference fields.

Note: As a good practice, make JavaScript calls to functions in a script include instead of a global business rule.

An example of an encoded query string is vendor=true, which returns all companies that are designated as vendors. Entering this string is the same as using the condition builder as shown in the example for the simple reference qualifier. For additional information on valid encoded query string syntax and examples, see Encoded query strings.
Advanced reference qualifier examples

An example of a JavaScript call is `javascript:new myScriptInclude().my_refqual()`. This code calls the function `my_refqual()` in the script include `myScriptInclude()`. The function must return a query string that can filter the options available on a reference field.

**Note:** You can also use encoded JavaScript filters such as `javascript:'u_active=true^' + "u_hr_service="+current.hr_service` in reference qualifiers.

In another example, if you are trying to filter based on the current company, you don’t have use a lookup script but can simply add this line to your dynamic qualifier:

```javascript
return "company=" + current.company;
```

You can also simplify this and use an advanced reference qualifier instead of a dynamic one:

```javascript:"company=" + current.company
```
Related lists and reference qualifiers

When a field appears on multiple related lists on a single form view, it may be necessary to validate which related list is being referenced to properly build the reference qualifier for the field. In this situation, configure the list control for the related list and enter a unique tag in the List edit tag field. This tag value is available to filter scripts as a variable named listEditRefQualTag. The following script include code is an example of a function that uses this type of tag.

```javascript
// Advanced reference qualifier on the CI Relationship Child field that takes into account // the related list that we are editing the child field on, if the field is being edited // from a tagged related list.

cmdb_rel_ci_child_refQual:function(){
  if(listEditRefQualTag =="application") return "sys_class_name = cmdb_ci_appl";
}
```
Using Javascript current syntax in reference qualifiers

current is a JavaScript object that contains the fields and field values of the active (current) record. For forms, this is the record that is displayed (loaded) in the form. Within advanced and dynamic reference qualifiers, you can use the JavaScript current object to define filters such as javascript:”company=” + current.company.

This JavaScript, within a reference qualifier, only returns the records from the referenced table that are equal to the company field value of the current record. So, if the value that appears in the Company field is Acme, the JavaScript returns all reference field records whose company value is equal to Acme (company=“Acme”). If you then bring up a record whose company value is “ViewRite”, the JavaScript resolves to company=“ViewRite.”

All fields within the currently loaded form (tables) are available for use with the current object. Use dot-walking to access values in a table, including the referenced table. For example, on the Incident form, the Assigned To field references the User table. To access the email address of the user, use the following syntax: javascript:”emailAddress=” + current.assigned_to.email.

Configure reference qualifiers

System administrators can configure reference qualifiers that enable filtering of the associated reference field.

This task walks you through creating a reference qualifier in the system dictionary. When creating a reference qualifier in the system dictionary, it not only applies to that table, but also to all the children of the table.

Note: You can also create reference qualifiers on extended tables through dictionary overrides. Dictionary overrides only impact the extended table and any of its children, not the parent table.

1. Navigate to the reference field on the form or table on which you want to define a reference qualifier.
2. Right-click the reference field label and select Configure Dictionary.

   The simple reference qualifier is available in both the default view and the advanced view. The dynamic and advanced reference qualifiers are available only in the advanced view.

4. In the Reference Specification section, verify that the table in the Reference field contains the table that you want associated with the reference field, or select another table if necessary.
5. From the Use reference qualifier choice list, select the reference qualifier to implement.
6. Configure the qualifier based on the type of reference qualifier.

   • Simple: Build the condition using the choice lists.
   • Dynamic: Either select an existing dynamic filter option or define a new dynamic filter option.
   • Advanced: In the Reference qual field, enter an encoded query string, JavaScript that returns a query string, or the name of a script include or business rule to run.

7. Complete the Reference Specification — Additional Customization section, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reference key</td>
<td>Identifies a field other than sys_ID to use as the unique identifier for the reference field.</td>
</tr>
</tbody>
</table>
### Field Description

**Reference cascade rule**

Defines what happens to a record if the record it references is deleted. Possible options include:

- None
- Cascade
- Clear
- Delete
- Delete no workflow
- Restrict

**Reference floats**

Flag that determines whether to configure the edit option for one-to-many relationships.

**Dynamic creation**

Flag that determines if the system should create a new record when a value for the reference field does not match an existing record. If you select this option, enter a script that specifies how to create the record in the **Dynamic creation script** field.

---

8. Click **Update**.

Constrain the assigned to field by role

This example shows how to use JavaScript and a business rule to restrict the incident **Assigned to** field choices to only the users with the `itil_admin` role.

Role required: personalize_dictionary or admin

You can also change `itil_admin` to any other role on a reference field that refers to the User table.

1. Open an incident.
2. Right-click the **Assigned to** field and select **Configure Dictionary**.
3. In the **Reference qual** field, enter
   
   javascript:"sys_idIN"+getRoledUsers("itil_admin").join(",").

4. Save the record.
5. To see the base system business rule that this JavaScript code calls, navigate to **System Definition > Business Rules**.
6. Open **getRoledUsers**.

   The business rule uses the following JavaScript code.

   ```javascript
   // Return an array of sys_ids of the users that have at least one role
   // optional parameters allow the exclusion (NOT IN) of some roles or
   // look for specific roles (IN)
   //
   // optional: queryCondition - 'IN' or 'NOT IN'
   // optional: roleList - a comma separated list of role names
   //
   function getRoledUsers(queryCondition, roleList) {
     var roleListIds;
     if (queryCondition && roleList) {
       roleListIds = getRoleListIds(roleList);
     }

     var users = {};
     var now_GR = new GlideRecord('sys_user_has_role');
     if (roleListIds) {
       now_GR.addQuery('role', queryCondition, roleListIds);
     }
     now_GR.query();
   }
   ```
Constrain the assignment group field

This example shows how to use an advanced reference qualifier with JavaScript and a script include to restrict the incident Assignment group choices to only the groups that contain the user specified in the Assigned to field.

Role required: personalize_dictionary or admin

1. Open an incident.
2. Right-click the Assignment group label and select Configure Dictionary.
3. If the form appears in Default view, under Related Links, click Advanced view.
4. In the Use reference qualifier field, ensure that the Advanced option is selected.
5. In the Reference qual field, enter javascript:new ReferenceQualifierHelper().backfillAssignmentGroup().
6. Save the record.
7. Navigate to System Definitions > Script Includes.
8. Click New.
9. Create a script include with the following JavaScript code. Ensure that the Accessible form field is properly set for the environment.

```javascript
var ReferenceQualifierHelper = Class.create();
ReferenceQualifierHelper.prototype = {

  backfillAssignmentGroup:function() {
    var assigneeGroupsQualifier = '';
    var assignee = current.assigned_to;

    //return if the assigned_to value is empty (this causes all groups to be returned)
    if(!assignee)
      return;

    //sys_user_grmember has the user to group relationship
    var grAssigneeGroups = new GlideRecord('sys_user_grmember');
    grAssigneeGroups.addQuery('user',assignee);
    grAssigneeGroups.query();

    while (gr.next()) {
      assigneeGroupsQualifier = assigneeGroupsQualifier + 'IN',assignee + ',
    }

    return assigneeGroupsQualifier;
  }

  // get sys_id's for the named roles
  getRoleListIds: function(roleList) {
    var ids = [];
    var now_GR = new GlideRecord('sys_user_role');
    now_GR.addQuery('name','IN',roleList);
    now_GR.query();
    while (now_GR.next()) {
      ids.push(now_GR.sys_id.toString());
    }
    return ids;
  }
}
```
while (grAssigneeGroups.next()) {
    if (assigneeGroupsQualifier.length == 0) {
        // Create the beginning of the qualifier and add the 1st group
        assigneeGroupsQualifier = 'sys_idIN' +
        grAssigneeGroups.getValue('group');
    } else {
        // build a comma separated string of groups if there is more than one
        assigneeGroupsQualifier += (',' + grAssigneeGroups.group);
    }
} // return Groups where assigned to is in those groups we use IN for lists
    gs.log('DP: RefQual = ' + assigneeGroupsQualifier);
    return assigneeGroupsQualifier;
}

To test, create an incident and select a user in the Assigned to field. Click the Assignment group lookup icon. Only the groups that contain the user you selected appear. For example, you assign an incident to Bob Smith, who belongs to the Database group and the Networking group. The only options that appear in the assignment group are Database and Networking.

The INSTANCEOF operator in reference qualifiers
You can use the INSTANCEOF operator in a reference qualifier to shorten or simplify a complex class qualifier.

For example, use the INSTANCEOF operator for a reference field to the cmdb_ci table to specify that all subclasses of a class are included in the results. The following reference qualifier returns all servers, including Linux, UNIX, Windows, and so on, because each of those subclasses extend the cmdb_ci_server class.

```
sys_class_nameINSTANCEOFcmdb_ci_server
```

In another example, you can simplify the following reference qualifier in a similar way.

```
u_active=true^sys_class_name=cmdb_ci_acc
^ORsys_class_name=cmdb_ci_computer
^ORsys_class_name=cmdb_ci_server
^ORsys_class_name=cmdb_ci_win_server
^ORsys_class_name=cmdb_ci_unix_server
^ORsys_class_name=cmdb_ci_linux_server
^ORsys_class_name=cmdb_ci_appl
^ORsys_class_name=cmdb_ci_netgear
```

Using the INSTANCEOF operator, the reference qualifier is rewritten as follows because the server subclasses extend the cmdb_ci_computer class.

```
u_active=true^sys_class_name=cmdb_ci_acc
^ORsys_class_nameINSTANCEOFcmdb_ci_computer
^ORsys_class_name=cmdb_ci_appl
^ORsys_class_name=cmdb_ci_netgear
```

Auto-complete for reference fields
By default, a reference field auto-completes as the user types in the field.

Administrators can configure additional auto-complete options. A user must have table-level read permission on the referenced table for auto-complete to display any options.
Dictionary attributes for auto-completion of reference fields

There are dictionary attributes that are specific to reference fields and that determine auto-complete behavior.

**Reference field auto-completion dictionary attributes**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
</table>
| ref_auto_completer | Specifies the name of the client-side JavaScript class that creates the drop-down auto completion choices. Valid class values include:  
  - **AJAXReferenceCompleter**: Displays matching auto-complete choices as a drop-down choice list. The list only displays the reference table's display value column. Reference fields automatically use this class if there is no other auto-completion class specified.  
  - **AJAXTableCompleter**: Displays matching auto-complete choices as rows in a table. The table displays the reference table's display value column and any columns listed in the `ref_ac_columns` attribute.  
  - **AJAXReferenceChoice**: Displays matching auto-complete choices as a drop-down choice-list. The list only displays the reference table's display value column. Furthermore, the list only displays up to 25 matching choices. If there are more than 25 auto-complete choices, the reference field instead displays the choices with the AJAXTableCompleter class. |
| ref_ac_columns    | Specifies the list of reference table columns to display. Separated column names with a semi-colon. For example, `ref_ac_columns=user_name;email;sys_created_on` allows auto-complete to match text from the user_name, email, and sys_created_on columns. |
| ref_ac_order_by   | Specifies the reference table column that sorts the auto-completion choices. For example, `ref_ac_order_by=name` sorts the auto-completion choices alphabetically by name. |

Administrators can also set a user preference to use a **contains** auto-complete search.

**Auto-complete UI features**

The AJAX table completer class has a number of UI improvements.
- The table completer always displays the number of records the auto-complete query finds.
- The table completer highlights the entire selected row by changing the color of the background and text.
- The table completer lists a value for every column.
  - The first time a value appears in a column, the table completer displays it in black text.
  - The table completer displays subsequent duplicate values in grey text. Previously, the table completer displayed an empty cell in a column containing a duplicate value.

```
Assigned to  b
Showing 1 through 4 of 4
Bow Ruggeri  Development
Bernard Laboy  IT
Beth Anglin  IT
Bud Richman  Sales
```

Selected row highlight

Set the `ref_autoCompleter=AJAXTableCompleter` dictionary attribute to use these improvements.

Define auto-complete attributes for all references to a table
A field inherits and uses the reference table's auto-complete attributes unless the field has its own value for the same attributes. You can define the attributes for references to a table, and it affects every form that references that table.

Role required: personalize_dictionary

A field-level attribute overrides a table-level attribute of the same name. If a field uses different reference attributes from those that are defined for the reference table, then the field uses both sets of attributes.

Use these steps to define auto-complete attributes for all fields in a table that do not already have their own auto-complete attributes. This example describes how to define auto-complete attributes for all references to the User [sys_user] table.

**Note:** A field's auto-complete attribute value supersedes a table's auto-complete attribute value. This means that any existing field-level value for an auto-complete attribute supersedes any value the administrator applies to the auto-complete attribute from the reference table.

1. Navigate to a list of the target table, such as **User Administration > Users**.
2. Perform the appropriate action for your list version.

<table>
<thead>
<tr>
<th>Version</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>List v2</td>
<td>Right-click the column header and click <strong>Configure &gt; Dictionary</strong>.</td>
</tr>
<tr>
<td>List v3</td>
<td>Open the list title menu and click <strong>Configure</strong>, and then click <strong>Dictionary</strong>.</td>
</tr>
</tbody>
</table>

3. Select the row that does not list a column name.
This row is typically the first row in the list. For example, select the first **sys_user** link.
4. Under **Related Links**, click **Advanced view**.
5. In the Attributes field, enter a comma-separated list of auto-complete attributes you want to apply to all fields in the table.
   For example, to display the user's department with all references to the sys_user table, enter:

   
   ```
   ref_auto_completer=AJAXTableCompleter,ref_ac_columns=department,ref_ac_order_by=department
   ```

6. Click Update.

To test the new auto-complete attributes, open a form that references the User [sys_user] table, such as an open incident. Enter a single character in the Assigned to field. The auto-complete options now include both the user name and department.

![Assigned to auto-complete options](image)

Remove the display value column
You can remove the display value column from a reference field by setting the `ref_ac_display_value` attribute to false.

Role required: personalize_dictionary
This causes the reference field to remove the display value column and only display the columns listed in the `ref_ac_columns` attribute. This feature requires the use of the AJAXTableCompleter class and the `ref_ac_columns, ref_ac_columns_search`, and `ref_ac_display_value` attributes.

![Auto-complete note](image)

This example describes how to remove the display value column from references to the User [sys_user] table and replace it with references to the first_name and last_name columns.

1. Navigate to a list of the target table, such as User Administration > Users.
2. Perform the appropriate action for your list version.

<table>
<thead>
<tr>
<th>Version</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>List v2</td>
<td>Right-click the column header and click Configure &gt; Dictionary.</td>
</tr>
<tr>
<td>List v3</td>
<td>Open the list title menu and click Configure, and then click Dictionary.</td>
</tr>
</tbody>
</table>

3. Select the row that does not list a column name.
   This row is typically the first row in the list. For example, select the first sys_user link.
5. In the Attributes field, add the `ref_auto_completer, ref_ac_columns, ref_ac_columns_search`, and `ref_ac_display_value` attributes.
   For example, to hide the display value column and only display the user's first and last names enter the following:

   ```
   ref_auto_completer=AJAXTableCompleter,ref_ac_columns=first_name;last_name,ref_ac_order_by=first_name
   ```
6. Click **Update**.

To test the new auto-complete attributes, open a form that references the User [sys_user] table, such as an open incident. Enter a single character in the **Assigned to** field. The auto-complete options now hide the display value column (user_name) and only display the first_name and last_name columns.

![Assigned to auto-complete options](image)

**Improve auto-complete queries**

By default, all reference fields use a `starts with` query to search for matching text in the reference table. This prevents auto-complete from executing inefficient `contains` queries every time a user searches a reference field. You can require all reference fields to use a `starts with` query.

Role required: admin

The following example illustrates a `contains` query. Note that the letter "d" appears anywhere in the user's first or last name.

![Assigned to search filter](image)

This procedure describes how to change the `glide.ui.ref_ac.startswith` system property to always use a `starts with` query.

1. In the navigation filter, enter `sys_properties.list` and press the Enter key.
2. Select the `glide.ui.ref_ac.startswith` property.
   To search for the property, enter `*startswith` in the Go to search filter for the **Name** column.
3. In the **Value** field, replace `false` with `true`.

   **Note:** Setting the `glide.ui.ref_ac.startswith` system property to `true` overrides any existing `autocomplete.contains` settings in both user and system level preferences. This property changes the autocomplete query method for all users regardless of preferences.

4. Click **Update**.
5. Test the change by opening a record with a reference field and entering a character in it, as illustrated in the example below.

![Assigned to field with auto-complete search](image)

**Configure auto-complete to match text from any reference field**

By default, auto-complete only matches text in the display value column. You can configure a reference field to match text from any additional column the reference field displays.

Role required: personalize_dictionary

You can add the `ref_ac_columns_search` attribute to enable auto-complete to match text in any column listed in the `ref_ac_columns` attribute. Set the `ref_ac_columns_search` attribute to `true` to match text from all reference field columns. By default (or when this attribute is `false`) auto-complete only matches text in the display value column.

1. Right-click the label of a reference field.
2. Select Configure Dictionary from the choice list.
4. In the **Attributes** field, add the desired auto-completion attributes. For example, these attributes add the department field to the caller list and sort callers by their department:

```
ref_auto_completer=AJAXTableCompleter, ref_ac_columns=department, ref_ac_order_by=department
```

5. Click **Update**.

The following example describes how to set the **Configuration Item** field display the CI class names from auto-complete choices for the Configuration item [cmdb_ci] table.

```
ref_auto_completer=AJAXTableCompleter, ref_ac_columns=sys_class_name, ref_ac_order_by=sys_class_name, ref_contributions=task_show_ci_map ; ci_show_incidents
```

*Note:* The **ref_contributions** attribute controls the icons that appear next to the reference field.
Enable contains auto-complete searches

By default, the reference auto-complete uses a **starts with** search. A user preference can be created to implement a **contains** search.

Role required: admin

1. Disable the `glide.ui.ref_ac.startswith` system property.
   
   For more information, see Improve auto-complete queries.

   **Note:** Setting the `glide.ui.ref_ac.startswith` system property to **true** overrides any existing "autocomplete.contains" settings in both user and system level preferences. This property changes the auto-complete query method for all users regardless of preferences.

2. Navigate to **User Administration > User Preferences**.
3. Select the preference """"<referenced table>.autocomplete.contains"""".
4. Set the **value** field to **true**.

5. Click **Update**.

Log out and log back in to display the updated search.

*Wildcards in reference auto-completes*

Wildcard searches use the auto-complete functionality.

Use an asterisk in the reference field for wildcard searches.

**One asterisk wildcard search**

If two asterisks are entered, a list of available records display in the auto-complete suggestions.
Two asterisk wildcard search

Recent selections

Reference fields store a list of each user's recent selections to allow users to quickly select past values when filling in a reference field.

By default, the system stores up to 15 selections from a reference field for each user in the Recent Selection [sys_ui_recent_selection] table. Users can see the recent selections list by selecting an empty reference field.

Note: The system does not store recent selections for service catalog reference variables.

Note: Recent selections are not available in the service portal or mobile user interfaces.

The system uses auto-complete to filter the list of recent selections to match values the user enters.
The system adds a Recent Selection record whenever a user inserts or updates a reference field value. Administrators can control the number of recent selections the system displays with the `glide.xmlhttp.max_choices` system property. Setting the property to zero disables recent selections.

**Note:** This property also controls how many entries the system displays in choice lists.

**Suggestion field type**

To help users find what they are looking for, you can add a suggestion field to any form.

Role required: personalize_dictionary

1. Open the form to which you are adding a suggestion field.
2. Add a new field or locate an existing field.
3. Right-click the field label and select Configure Dictionary.
4. In the Choice field, select Suggestion.
5. Click **Update**.

Suggestions are presented to the user.

Configure suggested text for string fields

You can configure the suggested text options for string fields.

Role required: personalize_choices

1. Right-click the field label and select **Configure Choices**.
2. Using the slushbucket, select options and the order in which you want them to appear.
   - To create a new option, enter the suggested text in the **Enter new item field** and click **Add**.
- The **Apply to Table** field is available when the current table extends another table (for example, Incident extends Task). This field allows suggested text options to be configured for all tables that extend the parent or for only the current (child) table.

3. Click **Save**.
4. To edit existing options, right-click the field label and select **Show Choice List**.

---

**Configure suggested text for journal fields**

You can configure the suggested text options for journal fields, such as work notes or the activity stream. Suggested text options for journal fields are unavailable in UI16.

Role required: personalize_responses

1. Right-click the field label and select **Configure Responses**.
2. Click **New**.
3. Enter a label, or brief description, for the option.
4. Enter the complete text in **Response text**.
5. Click **Save**.
Wiki field type

Wikitext fields use the basic wiki markup language and support links to external URLs and to sources within the system.

Some fields in the base system support Wikitext and administrators can add Wikitext fields on any form in the system.

Supported wiki tags

Basic tags are supported for Wikitext fields in the system.

<table>
<thead>
<tr>
<th>Format</th>
<th>Wiki tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>Headers</td>
<td>= Header 1 =, == Header 2 ==, etc.</td>
</tr>
<tr>
<td>Numbered step</td>
<td>#Step 1</td>
</tr>
<tr>
<td>Bullets (multi-level)</td>
<td>*Bullet 1, **Bullet 2</td>
</tr>
<tr>
<td>Indentation</td>
<td>:Level 1, ::Level 2</td>
</tr>
<tr>
<td>Line break</td>
<td>&lt;br&gt;</td>
</tr>
<tr>
<td>Format</td>
<td>Wiki tag</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Tables</td>
<td>Full table support, including cell spacing, padding, borders, background shading, and width measurements. For example:</td>
</tr>
<tr>
<td></td>
<td>{</td>
</tr>
<tr>
<td></td>
<td>! Header 1</td>
</tr>
<tr>
<td></td>
<td>! Header 2</td>
</tr>
<tr>
<td></td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>row 1, cell 1</td>
</tr>
<tr>
<td></td>
<td>row 1, cell 2</td>
</tr>
<tr>
<td></td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>row 2, cell 1</td>
</tr>
<tr>
<td></td>
<td>row 2, cell 2</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Sortable tables are not supported (class=&quot;sortable&quot;).</td>
</tr>
<tr>
<td>Code blocks</td>
<td>&lt;pre&gt; Generic block &lt;/pre&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;javascript&gt; Javascript Syntax &lt;/javascript&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;xml&gt; XML Syntax &lt;/xml&gt;</td>
</tr>
<tr>
<td>Bold</td>
<td>'''text'''</td>
</tr>
<tr>
<td>Italics</td>
<td>&quot;text&quot;</td>
</tr>
<tr>
<td>Ignore Wiki and HTML formatting</td>
<td>&lt;nowiki&gt; wikitext &lt;/nowiki&gt;</td>
</tr>
<tr>
<td>Web link</td>
<td><a href="http://community.service-now.com/">http://community.service-now.com/</a></td>
</tr>
<tr>
<td>Placed images</td>
<td>[[Image:&lt;image name&gt;]] For more information on uploading images or files to the database, see Storing images in the database.</td>
</tr>
<tr>
<td>HTML</td>
<td>Most common HTML tags are supported &lt;b&gt;bold&lt;/b&gt;, &lt;strong&gt;strong&lt;/strong&gt;, &lt;i&gt;italics&lt;/i&gt;, &lt;h1&gt;header1&lt;/h1&gt;, &lt;h2&gt;header2&lt;/h2&gt;, &lt;h3&gt;header3&lt;/h3&gt;, &lt;p&gt;paragraph&lt;/p&gt;, &lt;sub&gt;sub&lt;/sub&gt;, &lt;sup&gt;sup&lt;/sup&gt;, &lt;center&gt;center&lt;/center&gt;</td>
</tr>
</tbody>
</table>

### Create a Wikitext field

You can create a Wikitext field on any form.

Role required: personalize_form

1. Create a new field with the **Type** set to **Wiki**.
2. Click **Wikitext** to begin editing.

The Wikitext field appears on the form.

**Extend the functionality of a Wikitext field**

Configure the Wikitext field to link to other sources within the system.

Role required: personalize_dictionary

1. Right-click in the header of the new Wikitext field.
2. Select **Configure Dictionary**
3. In the **Dependent** field of the dictionary form, enter the field you want to use for linking to other pages.

For example, on the Incident table, you might choose the **number** field.
This configuration enables you to link to any incident by using that incident's number. For example, to open INC0000002, you enter \[\{INC0000002\}\].

The following dictionary attributes are available for wiki_text fields.

- **preview_first=true** - sets the preview mode to display on page load, otherwise editor will be displayed
- **preview_selector=true** - enables the toggle button to switch between the editor and preview
- **dual_mode=true** - enables displaying both the editor and the preview simultaneously during edit mode.

**Add and customize a field in a table**

Administrators can add new fields to a table to store and display data.

Role required: admin

**Warning:** Do not add more than 10 medium-length or longer String fields to a single table. Attempting to save a large number of characters in 11 or more String fields can result in the following error: Syntax Error or Access Rule Violation detected by database (Row size too large (> 8126).

1. Navigate to any form.
2. Right-click the form header and select **Configure > Form Layout**.
3. In the **Create new field** section, fill in the following fields:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the field as you want it to appear on forms and lists.</td>
</tr>
<tr>
<td>Type</td>
<td>Select a field type.</td>
</tr>
<tr>
<td>Field length</td>
<td>Select a field length. This field is visible only for certain field types.</td>
</tr>
</tbody>
</table>

4. Click **Add**.
5. Use the slushbucket to place the field in the desired location on the form.
6. Click **Save**.

The field now appears on the form in the designated location.

**Make a field mandatory**

Fields can be marked as mandatory, meaning they must contain a value before the record can be saved. Mandatory fields are marked with a field status indicator before the label.

Role required: personalize_dictionary

A mandatory field that is pre-populated by the platform with default data, such as a value from a client script, does not display the indicator. If you delete this value from the field, however, the indicator appears. The color of the indicator depends on the field state.

Using a dictionary entry to make a field mandatory does not work when using WebServices. You can use a data policy instead. For more information on data policies, see Data policy.

1. Right-click the field's label in the form and select **Configure Dictionary**.
2. In the **Dictionary** form, select the **Mandatory** check box.
3. Click **Update**.

   The next time the form is opened, a field status indicator appears next to the field label, indicating that a value is mandatory. If the mandatory field is pre-populated for any reason, the mandatory field indicator does not appear.

   **Note:** Mandatory fields are global. The field is marked as mandatory everywhere it appears in a form.

   **Note:** Making a **True/False** mandatory will have no effect. **True/False** fields are always considered to have a value. A selected check box has a value of true and an unselected check box has a value of false. Either of these values satisfies the requirement of a mandatory field.

**Mandatory Reference Fields**

A form can be saved with an empty mandatory field if that field is a reference field, and if the parent field is also blank. However, if the mandatory reference field shows a value from the parent field, then the form cannot be saved if this value is deleted. If the value in the referenced field is changed, the value for that field is changed everywhere it appears.

**Change the field label or hint**

You can change a field's label or the text that appears as a hint when you point your cursor to the field.

Role required: personalize_dictionary

1. Navigate to the form the field appears on.
2. Right-click the field label and select **Configure Label**.
3. Update the form.

**Changing the Field Label or Hint**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>The table the label appears on.</td>
</tr>
<tr>
<td>Label</td>
<td>The label that the field displays. You can enter up to 80 characters for the label, but not all databases support this many characters. The recommended maximum is 30 or fewer characters. HTML in field labels is not supported.</td>
</tr>
<tr>
<td>Plural</td>
<td>The plural version of the field label.</td>
</tr>
<tr>
<td>Element</td>
<td>The dictionary name of the field.</td>
</tr>
<tr>
<td>Help</td>
<td>Helpful text stored in the record.</td>
</tr>
<tr>
<td>Hint</td>
<td>A short description of the field that displays when the user hovers over it.</td>
</tr>
<tr>
<td>URL</td>
<td>A URL link that displays on the label if this field is not blank.</td>
</tr>
<tr>
<td>URL target</td>
<td>A target attribute that determines where the URL will open. For information on the target attributes, see this W3Schools article.</td>
</tr>
</tbody>
</table>

4. Click **Update**.
Delete a field from a table

You can delete custom fields that you created. Custom fields begin with u_. It is recommended that you remove the field from forms and lists instead of deleting it.

Role required: admin

You cannot delete base system fields. In addition, any missing base system fields are recreated when the instance is upgraded.

1. Navigate to a form that contains a custom field to delete.
2. Right-click the field label and select Configure Dictionary.
3. Click Delete Column in the form header, and then click OK.
4. To delete multiple custom fields, complete the following steps.
   a) Navigate to System Definition > Dictionary.
   b) Locate the custom fields to delete.
      For example, search for column names that start with u_.
   c) Check the boxes next to the fields to delete and select Delete from the action list below the list.
      A confirmation dialog opens and reminds you that this may result in deletion of related records. If there are dependencies for the selected fields, they are listed.
   d) To proceed, click Delete.

Add users to a watch list

Watch lists allow multiple users to subscribe to notifications of a task. Expand the watch list and select users with the glide controls.

Role required: none

1. Expand the watch list by clicking the lock icon (🔒).
2. Select users with the glide list controls (see table).

<table>
<thead>
<tr>
<th>Glide controls</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Icon</strong></td>
</tr>
<tr>
<td>🗝️</td>
</tr>
<tr>
<td>✗</td>
</tr>
<tr>
<td>🔄</td>
</tr>
<tr>
<td>🗃️</td>
</tr>
<tr>
<td>🗃️</td>
</tr>
<tr>
<td>🔍</td>
</tr>
</tbody>
</table>
Configure email notifications for watch lists

Watch lists (glide_list field type) allow multiple users to subscribe to notifications of a task. You can specify conditions in an email notification to send email notifications to the members when the conditions are met.

Role required: admin

To receive these notifications, users must define an email address in their user record or enter an email address into the watch list email field.

Important: Administrators configure email notifications for watch lists (see Configure email notifications for watch lists).

An advanced configuration using watch lists involves placing two watch lists on a form, one for the general comments on a task and another for work notes or non-public comments. By configuring separate email notifications, separate users on each watch list can be notified about different information.

If users on a watch list are getting more than one email for each update to an incident, it can be because other recipients are replying all to an email notification. Recipients may be receiving email through their email system (Outlook, Groupwise, and so on) and through the base system. To stop this duplication, remove the names of other users from the email or the watch list.

1. Open the notification to configure.
2. In the Who will receive section, select the icon beside Users/groups in fields.
3. Double-click Watch list in the Available column to move it to the Selected column.
4. Click Update.

Hide email addresses in a watch list

You can remove the email address text entry element from a watch list by modifying the dictionary.

Role required: admin

1. Open a task record that displays the Watch list field.
2. Right-click the label and select Configure Dictionary.
3. In the Attributes related list, click New.
4. Enter or select the no_email attribute and enter true in the Value field.
5. Click Submit.

The email entry field is hidden. Users can select users from the reference field to add to the watchlist.

Configure order buttons on the watch list slushbucket

When you add multiple users to a glide_list, such as a watch list, the slushbucket does not display the order buttons for the list of selected members. You can set a dictionary attribute to display the order buttons.

Role required: admin

The slushbucket opens when the user clicks the add/remove multiple users icon.
By default the order buttons on the right are not displayed. Follow the procedure to display the order buttons.
1. Open a task record that displays the **Watch list** field.
2. Right-click the label and select **Configure Dictionary**.
3. Under **Related Links**, click **Advanced view**.
4. In the **Attributes** field, enter `maintain_order=true` separated by a comma if necessary.
5. Click **Update**.

**Highlight list fields**

Color fields in lists to call an agent's attention to them.

Role required: admin

Highlighted fields in lists appear colored and optionally, have a leading bullet.
The set up involves specifying the fields that gets highlighted and the conditions that trigger the highlighting.

**1. When you list records from this table**

**2. Highlight this field in each record**

**Priority = 1 - Critical**

**3. Where this condition is true**  
100  true

Available highlighting colors are:

- Critical
- High
- Warning
- Moderate
- Positive
- Info
- Low

You cannot highlight the following field types:

- Reference
- URL
• Document IDs

1. Navigate to Workspace Experience > Administration > Highlighted Values and click New.
2. On the form, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>Name of the table that contains the fields you want to highlight.</td>
</tr>
<tr>
<td>Field</td>
<td>Name of the field you want to highlight if the triggering conditions are met.</td>
</tr>
<tr>
<td>Application</td>
<td>Scope of applications this highlighting pertains to.</td>
</tr>
<tr>
<td>Workspace</td>
<td>The workspace this highlighting applies to.</td>
</tr>
</tbody>
</table>

The **Field** value can be unrelated to the condition that triggers the highlighting. In the following example, if the **Caller** is Fred Luddy, Workspace highlights the **Priority** field, not the **Caller** field.

3. Right-click the header and click **Save**.
   You've specified the field where the highlights appear. Now, it's time to specify the conditions that trigger the highlighting.

4. In **Highlighted Value Conditions**, click **New**.
5. In the Highlighted Value Condition form, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conditions</td>
<td>Conditions that trigger the highlighting. The condition can be different from the field that gets highlighted. For example, you might highlight the <strong>Priority</strong> field in a record if the <strong>Caller</strong> in that record is Fred Luddy. A simpler example is highlighting the <strong>Priority</strong> field if the priority value is <strong>critical</strong>.</td>
</tr>
<tr>
<td>Status</td>
<td>The highlighting color.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Show Icon</td>
<td>Toggle to display (selected) or hide the leading bullet when highlighting.</td>
</tr>
<tr>
<td>Value Override</td>
<td>Text that replaces the field values from the table. If you don't supply a Value Override, Workspace highlights the field value from the table. If you supply a value, Workspace replaces the field value with your text and highlights that.</td>
</tr>
<tr>
<td>Application</td>
<td>Scope of applications this highlighting pertains to.</td>
</tr>
<tr>
<td>Order</td>
<td>The order in which to evaluate the conditions. When you have multiple conditions for highlighting the same field, they are evaluated in order from lowest to highest. If any of the conditions are True, Workspace highlights the field.</td>
</tr>
</tbody>
</table>

6. Click **Submit**.

In the following example, the highlighting was triggered on the **Priority** field because the priority value was critical.

<table>
<thead>
<tr>
<th>Number</th>
<th>Opened</th>
<th>Short description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INC0000002</td>
<td>2019-05-29 16:07:12</td>
<td>AGAIN UPDATED</td>
</tr>
<tr>
<td>INC0000031</td>
<td>2019-05-09 17:18:03</td>
<td>UPDATED VIA MULTI-EDIT</td>
</tr>
</tbody>
</table>

7. Optional: Click **New** on the **Highlighted Value Conditions** Related List and create another condition for highlighting the same field.

For example, highlight the **Priority** field associated with the Incident table when the **Priority** value is "critical," or when the **Caller** value is "Fred Luddy." The conditions are ranked according to the **Order** value. Workspace evaluates the lowest value first.

<table>
<thead>
<tr>
<th>Conditions</th>
<th>Order</th>
<th>Show Icon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority = 1 - Critical</td>
<td>30</td>
<td>true</td>
</tr>
<tr>
<td>Caller = Fred Luddy</td>
<td>50</td>
<td>true</td>
</tr>
</tbody>
</table>
8. Optional: Remove all highlighting from a filtered list that would otherwise have highlighting.

When setting up highlighting for a table, all filtered lists associated with the table display highlighted fields unless you disable highlighting for specific, filtered lists.

a) Navigate to `sys_aw_list.list`.

b) In the **Name** column, enter the name of the table with highlighted fields, for example, Incident. All filtered lists associated with the table appear.

c) Click the filtered list you want to remove highlighting from.

d) On the Workspace List form, if Global is the current application, click **here** in To edit this record click **here**.

e) Select the **Ignore Highlight in List** check box and click **Update**.

Now, regardless of the conditions, Workspace will not highlight any fields in the specified filtered list. This option does not work, however, for filtered lists in **My Lists**, which are the filtered lists agents create.

### Modify string field length

You can modify the maximum character limit for a string field.

**Role required:** personalize_dictionary

The URL type field hides the Max Length field on the Dictionary form by default. Browsers support URL length up to 2,083 characters. The URL field is a String field.

1. Right-click the field label in the form and select **Configure Dictionary**.

2. Change the **Max length** field to the desired length.

   **Note:** You can change between string-based data types as long as length changes do not cause any data loss from truncation. For example, you can change from a MEDIUM database type to a VARCHAR(100) database type if none of the existing data is greater than 100.

3. Click **Update**.

   The system cancels any length change that results in data loss due to truncation.

### Specify a default field value

A default value populates a value in a field when a new record is created.

**Role required:** personalize_dictionary

The default value populates the field on the blank form for a new record, and also subsequently when the new record is submitted if the field is empty. Default values can be specified as either a constant or generated through script.

1. Right-click the field's label in the form and select **Configure Dictionary**.

2. Enter the default value in the **Default value** field.

   To set a constant value, type it into the **Default value** text box field. To assign a default value using a more complex formula, use JavaScript to output a default value.

   **Note:** The default value should be the underlying value that would be present in the field, not the label. For example, in a choice list field, use the value of the choice as the default value, not the choice's name.
Default field value examples

Review the following examples about specifying default field values.

Constant default values

Here is an example that sets a default value for the **Priority** field.

![Dictionary Entry Priority]

**Default value constant**

Javascript default values

To view out-of-box examples of JavaScript default values, navigate to **System Definition > Dictionary** and enter this filter: **[Default value] [starts with] [javascript]**. Open some of the records and view the default value javascript entries.
Set a default value for assignment_group

The following example sets a default value in a [sys_user_group] reference field by getting the ID from the name of a group.

```javascript
javascript:GetIDValue('sys_user_group', 'Development');
```

Set a default value for assigned_to if user has the itil role

This example for the Task [task] table describes how to configure the default value for the [assigned_to] user equal to the current user id if the user has a role of itil.

- Column label: Assigned to
- Column name: [assigned_to]
- Reference Specification section
  - Reference: User [sys_user]
  - Reference qual condition: [Roles] [is] [itil]
- Default value script:

```javascript
javascript:if (gs.hasRole("itil"))current.assigned_to = gs.getUserId();
```

Set a default value for a duration field

To set a default value for a duration field, use the following in the Default value field of the duration field's dictionary entry:

```javascript
javascript:current.duration_field.setDisplayValue('3 04:30:14');
```

Avoid hard-coding a particular date-time. If the system date-time format changes, the value becomes invalid. Instead, select the Use dynamic default check box and assign a dynamic filter option. For more information on dynamic filters, see Create a dynamic filter option.

Make a field dependent

A choice or reference field can be declared dependent on another field on the same table. Dependent fields limit their available values based on the value in the dependent field.

Role required: personalize_dictionary

If a required dependency does not function as expected, as might happen if there is a many-to-many relationship between the fields, consider using reference qualifiers to accomplish the goal.

1. Right-click the field label in the form and select Configure Dictionary.
2. In the Dependent field, enter the name of the field that this field will depend on.
3. Click **Update** when done.

In the example below, the "subcategory" field is made dependent on "category". The "category" value in a form will determine which options appear for the "subcategory" field.

<table>
<thead>
<tr>
<th>Dictionary Entry</th>
<th>= Required field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table:</td>
<td>Incident [incident]</td>
</tr>
<tr>
<td>Column name:</td>
<td>subcategory</td>
</tr>
<tr>
<td>Type:</td>
<td>string</td>
</tr>
<tr>
<td>Choice:</td>
<td>Dropdown with -- None</td>
</tr>
<tr>
<td>Default value:</td>
<td></td>
</tr>
<tr>
<td>Attributes:</td>
<td></td>
</tr>
<tr>
<td>Dependent:</td>
<td>category</td>
</tr>
<tr>
<td>Table reference:</td>
<td></td>
</tr>
</tbody>
</table>

**Note:**
Fields cannot be made dependent on derived fields.

---

**Require unique values for a field**

The system allows you to require that a field's values be unique. When this is done, the system will not let two records have the same value for that field.

Role required: personalize_dictionary

By default, fields are created without this constraint. A field can have unique values only if there are not already duplicate values in the database for that field. The system does not allow you to make a field unique while there are duplicate values in the table.

1. Verify that no records in the table for the field have values, or that they all have the same value.
2. Right-click the field label in the form and select **Configure Dictionary**.
3. Configure the form to add the **Unique** field if it does not already appear.
4. Select the **Unique** check box.

5. **Update.**

**Define field styles**

Field styles allow you to declare individual CSS styles for a field in a list or form.

Role required: personalize_styles or admin

The CSS lets you change the following attributes of a field.

- Change the color.
- Change the font attributes (bold, italics, underline).
- Change the padding and alignment of text.

You can define field styles for tables and database views that are in the same scope as the field style and for other tables that have at least one field in the same scope as the field style. Field styles defined for a table do not apply to database views that include the table. Create separate field styles for database views.

**Note:** Field styles are not applied to comments and work notes fields used with the activity formatter. Background color for these fields can be set using the `glide.ui.activity_stream.style.comments` and `glide.ui.activity_stream.style.work_notes` system properties located in the `sys_properties` table.

1. Navigate to the list of styles for the field in one of the following ways.
   - Right-click the field label on the form and select **Configure Styles**.
   - Navigate to **System UI > Field Styles**, and locate the field to apply a style (admin only).

2. Click **New**, or click the style to modify.
3. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Input Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>Table that contains the field.</td>
</tr>
</tbody>
</table>

**Note:** The list shows only tables and database views that meet the scope protections for field styles.
<table>
<thead>
<tr>
<th>Field</th>
<th>Input Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field name</td>
<td>The field to which the style applies.</td>
</tr>
<tr>
<td>Value</td>
<td>The exact value or script-based-condition required to apply the style.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The value only affects list field styles. To apply field styles on both lists and forms, leave this field blank.</td>
</tr>
<tr>
<td>Style</td>
<td>The CSS style to apply. For example, to make the background of the Incident Category fields red in record lists, with a 24-px font size and white text color, enter the following code.</td>
</tr>
<tr>
<td></td>
<td>background-color:red; font-size:24px; color:white;</td>
</tr>
</tbody>
</table>

You can use a script-based-condition with the syntax `javascript:<script>` in the Value field to determine whether the system should apply a style to a field in the list. If the evaluated script returns true, the system applies the style to the list item.

The script has access to the current script object, which enables you to build conditions based on the field values of the current record. For example, this script checks for overdue items based on a field value:

```javascript
javascript: gs.dateDiff(gs.now(), current.u_datefield.getDisplayValue(), true) < 0
```

**Note:** In this example, `current.u_datefield` refers to the name of a custom date field.

The system only supports one `javascript:<script>` entry in a Value field. If you want to enter multiple JavaScript conditions, consolidate the conditions into one statement. For example, instead of this invalid entry:

```javascript
javascript: current.state == "Completed" javascript: current.error_tables > 0
```

Consolidate the conditions into one statement such as:

```javascript
javascript: current.state == "Completed" && current.error_tables > 0
```

4. Optional: To add alternative text for a style, configure the form to add the alternative text field.

   For styles like the VIP style icon, you can add alternative text so that screen readers can differentiate between the style and the text.

5. Click Submit or Update.
Record numbering

In the base system, several tables are numbered, including Incident, Problem, Change Request, and Knowledge. You can also use these numbers anywhere that script is present, for example to generate watermarks for emails. Records in tables can be numbered automatically.

Administrators can manage record numbering by navigating to **System Definition > Number Maintenance.** The current number format for a table, including the prefix (such as INC for incidents or CHG for changes), is stored in a record on the Number [sys_number] table.

![Number Maintenance Table](image)

**Number table**

You can renumber auto-incremented tables that extend the task table or manage numbering with a database field named **Number this field.** For information about renumbering custom tables, see KB0538764: Renumbering auto-incrementated custom tables in the ServiceNow knowledge base.

**Note:** If you reset numbering in Number Maintenance, it only renumbers new records. It leaves the numbering as-is for existing records in system tables.

**Add auto-numbering records in a table**

You can define one number format per table in the system.

Role required: admin

1. Navigate to **System Definition > Number Maintenance.**
2. Click a table name to view the number record for that table, or click **New.**
3. Define the number format by completing the fields (see table).
4. Click **Submit** or **Update.**

If an auto-numbered field does not already exist, a new field is automatically created on the table with the following values:

- Label: Number
• Name: u_number
• Default value:

```javascript
javascript:getNextObjNumberPadded();
```

**Note:** This script renumbers records when the Number of digits is updated. To use a script that does not renumber records when the Number of digits is updated, open the dictionary entry for the Number field and enter the following script in the Default value field.

```javascript
javascript:getNextObjNumber();
```

### Auto-numbering records in a table

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>Select a table.</td>
</tr>
<tr>
<td>Prefix</td>
<td>Enter a prefix for every number in the table (for example, INC for Incident).</td>
</tr>
<tr>
<td>Number</td>
<td>Enter the base number for this table (default value is 1000). Record numbers are automatically incremented, and the next number is maintained in the Counter [sys_number_counter] table. If you set the base number to a value higher than the current counter, the next record number uses the new base number. Otherwise the next record number uses the current counter. The counter does not reset to a base number lower than itself. To see the current counter, click the Show Counter related link.</td>
</tr>
</tbody>
</table>
| Number of digits | Enter the minimum number of digits to use after the prefix (default value is 7).  
  - Leading zeros are added to auto-numbers, if necessary. For example, INC0001001 contains three leading zeros.  
  - The number of digits can exceed the minimum length. For example, if Number of digits is 2 and more than 99 records are created on the table, the numbers continue past 100 (such as INC101). |

**Warning:** Changing this field may update all number values for existing records on a table. Take care when changing this field on a production instance.

**Note:** To change the default values for new number formats, change the Default value field on the system dictionary record for the Number or Number of digits field. These fields are on the Number table.
Prepare to left-pad number fields in custom tables

Before you configure left padding of number fields on a custom table or a table that does not extend the task table, you must prepare business rules and script includes.

Role required: admin

1. Duplicate the base system business rule named Pad Numbers: Click Insert and Stay. If Insert and Stay is not available on your instance, create a new business rule and manually copy all field values from Pad Numbers.
2. Give the business rule a new name and change the script field to read as follows:

```javascript
function padCurrentCategory()
    var target = new GlideRecord(current.category+"\n");
    if (!target.isValidField("u_number") || target.isValidField("number")) return;
    var nm = new UNumberManager();
    nm.padTableNumbers(current.category, current.maximum_digits);
} Save the changes.
```
3. Duplicate the base system script include named NumberManager.
4. Change the following two lines as indicated:

```javascript
105: currentNumber = records.u_number.toString();
117: records.u_number = prefix + currentNumber;
```
5. Name the new script include UNumberManager and save your changes.

You can now continue with the process of configuring left-padding and renumbering records.

Configure left padding of a system number in a table

You can configure the left padding of the system numbers on a table. For example, pad the Number field on an Incident, Problem, or Change Request.

If you are configuring numbers on a custom table or a table that does not extend the task table, then, before performing the following procedure, you must prepare business rules and script includes. For more information, see Prepare to left-pad number fields in custom tables.

Role required: admin

1. Navigate to the form, then right-click the Number field and select Configure Dictionary.
2. Enter the following script in the Default value field and click Update.

```javascript
g getNextObjNumberPadded();
```
3. Navigate to System Definition > Number Maintenance.
4. Open the table record.
5. Enter a value in the Number of digits field.
6. Click **Update**.

Number padding is applied to both existing and new records.

![Sys number](image)  
<table>
<thead>
<tr>
<th>Table:</th>
<th>incident</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number:</td>
<td>10,000</td>
</tr>
<tr>
<td>Prefix:</td>
<td>INC</td>
</tr>
<tr>
<td>Number of digits:</td>
<td>7</td>
</tr>
</tbody>
</table>

Update  Delete

The result of the configuration in the image is an Incident number that is left padded.

![Incident](image)

### Prevent numbering gaps

By default, numbers are generated every time a new record is created.

Role required: admin

When records are created but not saved, a gap in the numbering is created. You can prevent these numbering gaps by generating numbers only when records are saved.

1. Navigate to **System Properties > System**.
2. Set the property **Assign a task number only upon insert (prevents unused numbers)**, `glide.itil.assign.number.on.insert`, to `true`.
3. Click **Save**.

### Enforcing unique numbering

Although duplicate numbers are rare, numbering does not enforce uniqueness, by default.

To enforce uniqueness, you can:

- Create a before business rule on insert only to check for duplicate values and replace duplicates with the next available number.
- Enable a unique index on the table.

**Note:** While unique indexes ensure data integrity they also prevent any insert involving a duplicate number. This may cause unexpected errors during data entry.
Sample business rule

This sample script can be used as part of a before business rule on insert only to check for duplicate numbers and replace them with the next available number. The following script references a script created in Configure left padding of a system number in a table.

```javascript
var curNum = current.number + ''; 
if(curNum) {
    var recordClass = current.getRecordClassName();
    var now_GR = new GlideRecord(recordClass);
    gr.addQuery('number', curNum);
    gr.query();
    if(gr.getRowcount() > 0) { 
        var newNum = getNextObjNumberPadded();
        gs.addInfoMessage("The number "+ current.number + " was already used by another "+ recordClass + ". The " + recordClass + " number has been changed to " + newNum);
        current.number = newNum;
    }
}
```

Field normalization and transformation

Field Normalization includes normalization and transformation, which are two different ways to alter field values for increased data integrity and reduced duplication.

Normalization

Normalization searches for variations of the same field value and converts them into a single preferred value. By consolidating multiple variations of the same value into a single simple recognizable value, the system eliminates duplicate records and provides better search results. When a process or a user enters a value in a normalized field, the system determines whether to replace it with a normal value. Normalization also automatically adjusts queries to return normalized results and normalizes values in scripts.

While normalization is available for every field in the platform, it works best for descriptive values such as names or standard units of measurement. For example, you might create normalization rules to:

- Set the CPU type of a computer CI to a standard model name such as Xeon.
- Set the suffix used for the names of corporations to a standard format such as ServiceNow, Inc.

Transformation

Transformation converts raw field input values into standardized values that are more meaningful to an organization. Administrators control when transformation happens by defining rules and conditions for specific fields. For example, you might create transformation rules to:

- Remove suffixes from user names such as Jr. and II.
- Round computer CI RAM sizes to the nearest whole number such as rounding 4112 MB to 4000 MB.
Transform records make up the rules that define how a field transformation is executed. Order values determine the order in which each rule is evaluated. A check box on each transform enables an administrator to determine where processing stops when a rule evaluates to true.

**Enabling normalization and transformation by field type**

Field type records specify which data types are available for normalization and transformation. By default, the system supports normalization and transformation for these field types.

<table>
<thead>
<tr>
<th>Field type</th>
<th>Use to normalize</th>
<th>Use to transform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decimal</td>
<td>false</td>
<td>true</td>
</tr>
<tr>
<td>Float</td>
<td>false</td>
<td>true</td>
</tr>
<tr>
<td>Integer</td>
<td>false</td>
<td>true</td>
</tr>
<tr>
<td>Numeric</td>
<td>false</td>
<td>true</td>
</tr>
<tr>
<td>String</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>URL</td>
<td>true</td>
<td>true</td>
</tr>
</tbody>
</table>

A field type entry applies to all fields whose dictionary entry data type matches the field type entry. Administrators can create additional field type records for other data types as needed.

**Warning:** Avoid creating field type records for fields that store a Sys ID value such as a reference field, field name field, or a table name field. Directly altering a Sys ID value is more likely to produce data corruption and broken references than to produce meaningful standard values. Instead, normalize or transform the display value associated with the Sys ID. For example, normalize the user name instead of the Sys ID of a specific user.

**Identifying normalized fields**

The system displays the normalization icon on fields with an associated normalization or transformation record. Users with the normalizer role can click the icon to access the associated normalization or transformation record. Users without the normalizer role instead see a help page. Administrators can configure who sees the normalization icon with a preference called **Restrict to roles**.

**Activate Field Normalization**

You can activate the Field Normalization plugin (com.snc.field_normalization) if you have the admin role. This plugin includes demo data and activates related plugins if they are not already active.

Role required: admin

1. Navigate to **System Applications > All Available Applications > All**.
2. Find the plugin using the filter criteria and search bar.

   You can search for the plugin by its name or ID. If you cannot find a plugin, you might have to request it from ServiceNow personnel. For more information, see **Request a plugin**.

© 2021 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
3. Click **Install**, and then in the Activate Plugin dialog box, click **Activate**.

**Note:** When domain separation and delegated admin are enabled in an instance, the administrative user must be in the **global** domain. Otherwise, the following error appears: Application installation is unavailable because another operation is running: Plugin Activation for <plugin name>.

### Installed with field normalization

Several components are installed with Field Normalization.

The following preferences (**Field Normalization > Administration > Preferences**) control features for normalization and transformation:

<table>
<thead>
<tr>
<th>Field Normalization preferences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preference</td>
</tr>
<tr>
<td>Enable field normalization</td>
</tr>
<tr>
<td>Enable field normalization auditing</td>
</tr>
<tr>
<td>Logging</td>
</tr>
<tr>
<td>Decoration URL</td>
</tr>
<tr>
<td>Restrict decorations to roles</td>
</tr>
</tbody>
</table>
Normalization preferences

Business rules

The following business rules were created for this plugin:

- Ensure Rules Application Job
- Ensure Transform Application Job
- Ensure Rules and Alias Jobs
- Ensure Transform Application Job
- Ensure Decoration Attribute
- Cleanup on field or table change
- Prevent duplicates in class hierarchy
- Handle potential duplicates
- Run job
- Ensure Pending Value Collection Job
- Ensure name changer job
- Flush forms when activating

**Field Normalization roles**

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>normalizer</td>
<td>Person authorized to manage field normalization and transformation.</td>
</tr>
<tr>
<td>normalization_tester</td>
<td>Person authorized to create test records for normalizations and transformations. Only records opened by users with this role are available for testing normalization and transformation rules in Test mode.</td>
</tr>
</tbody>
</table>

**Field Normalization script includes**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FieldNormalizationAjax</td>
<td>Provides AJAX services for the Field Normalization plugin.</td>
</tr>
<tr>
<td>FNEnsureJob</td>
<td>Ensures that a job record exists for a particular extant data job target.</td>
</tr>
<tr>
<td>FNExtantDataJobChoices</td>
<td>Generates a list of tables for use in document_id field of the fn_extant_data_normalization table.</td>
</tr>
<tr>
<td>FNExtantDataJobUtil</td>
<td>Determines whether an extant data job is allowed to run.</td>
</tr>
<tr>
<td>FNFields</td>
<td>Returns valid fields for normalization.</td>
</tr>
<tr>
<td>FNTransformChooserUtil</td>
<td>Provides support for the fn_transform Chooser UI page.</td>
</tr>
<tr>
<td>Position</td>
<td>Finds a position within a given string.</td>
</tr>
<tr>
<td>Round</td>
<td>Rounds numbers with various rounding modes and intervals.</td>
</tr>
</tbody>
</table>

**Field Normalization UI pages**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aliases</td>
<td>Creates the slushbucket with pending values for choosing aliases for a normal value.</td>
</tr>
<tr>
<td>fn_transform Chooser</td>
<td>Displays available transforms. Invoked by the New button on the fn_transform related list.</td>
</tr>
</tbody>
</table>
Enable a field type for normalization or transformation

Create or modify a normalization field type record to enable a specific field data type for use with normalization or transformation.

To normalize or transform a value in a reference field, apply the processing to the field in the target table.

1. Navigate to Field Normalization > Administration > Normalization Field Types.
2. Click New in the record list.
3. Enter a Name for the field type that clearly describes the type in the dictionary.
   This value is for reference only and is not used in any processing. For example, you might enter IP Address for the field type of ip_address.
4. Enter the Type from the dictionary.
5. Select the appropriate check box to use this field type to normalize or transform fields.
   In the base system, only the String field type is used for normalization.
6. Right-click in the header bar and select Save from the choice list.
   The Transform Categories Related List appears.
7. If this field type is being used for transforms, click **Edit** to associate an existing Transform Category with this field type.

**Note:** If you create a custom field type that is used for normalizations only, a link to a transform category is not necessary.

The relationship of a field type to a category, and the category to a list of transformation definitions, is completely configurable.

The String field type is associated with the Text Transform Category, which contains these transform definitions. Any of these associations are configurable.
Create a raw field

A raw field is a custom field created by an administrator to show the original (raw) input in a field on a form after it has been normalized or transformed.

An administrator might add a custom field to a form to show the original, or raw, value of a normalized field.

This is a read-only field that might be called something like Raw CPU type or Original Name. In the following example, the CPU type field was normalized to Xeon from an original, raw value of Xeon L3350.

1. In the form containing the field that is being normalized or transformed, right-click in the header bar.
2. Select Personalize > Form Layout.
3. Complete the Create new field form at the bottom of the page, and then click Add.
   • Name: Type the field label. In this case, use Raw + <field label>.
   • Type: Select a data type from the list for this field.
   • Field length: Select the character limit for this field. The default is 40.
4. Move the new field adjacent to the normalized field using the direction arrows in the slushbucket.
5. Click Save.
### Normalization and transformation data jobs

The system uses data jobs to change field values during normalization and transformation.

Administrators must manually start data jobs that apply field changes. By default, which blocks administrators from running manual data jobs that apply changes to existing data. Most data jobs have a roll back option to revert changes after the job completes. By default, the system provides these data jobs.

#### Note:

If the Field Normalization plugin is active, the normalization engine executes on insert of records into a table according to normalization rules. To learn more about this plugin, see Activate Field Normalization.

If the Field Normalization plugin is not active, a data job runs to normalize the values. The data job saves the previous values in the rolled back fields to revert them if necessary.

<table>
<thead>
<tr>
<th>Name</th>
<th>Used for</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pending value collection</td>
<td>Normalization</td>
<td>The system runs this job to collect field values that will change during the next field normalization run. The system runs this job whenever you insert or update a field normalization record. Since this data job does not change any field values, there is no roll back option.</td>
</tr>
<tr>
<td>Normal value change</td>
<td>Normalization</td>
<td>Run this job to rerun field normalization and update field values when you change a normal value. The system creates this job whenever you change a normal value. Roll back the data job to revert the normalized fields to the previous normal value.</td>
</tr>
<tr>
<td>Alias application</td>
<td>Normalization</td>
<td>Run this job to normalize all field values that match an alias. The system creates this job whenever you create or update an alias. Roll back the data job to revert normalized fields to their previous values.</td>
</tr>
<tr>
<td>Rule application</td>
<td>Normalization</td>
<td>Run this job to normalize all field values that match a rule. The system creates this job whenever you create or update a rule. Roll back the data job to revert normalized fields to their previous values.</td>
</tr>
<tr>
<td>Coalesce too normal</td>
<td>Normalization</td>
<td>Run this job to normalize the reference field values by replacing references to multiple duplicate records with one reference to a normalized record. The system creates this job whenever you change a normal value that applies to a reference field. Roll back the data job to restore the duplicate records as valid options. The rollback does not restore references to the previous records.</td>
</tr>
</tbody>
</table>
### Run a single data job

Running the data job/jobs is the fourth step in transforming a field. This topic explains how to run a single data job.

1. Start the Transform application data job to apply the transform to all the appropriate records in the database.
2. Open the Transformation record and switch the Mode to Active.
3. Select the Data Jobs Related List.
4. Run the data job using one of the following methods.
   - In the list of data jobs, select the check box of the jobs you want to run, and then select Start from the Actions menu.
   - Click the link in the Created column to open the data job, and then click the Start Related Link.

The State of the jobs turns to Queued as it runs and to Completed when it finishes successfully.

### Run multiple data jobs

Running the data job/jobs is the fourth step in transforming a field. This topic explains how to run data jobs for multiple field transformations.

1. Start the Transform application data job to apply the transform to all the appropriate records in the database.
2. Navigate to Field Normalization > Data Jobs > All.
3. Select the check boxes for the jobs you want to start.
   - Note: These jobs must have the Mode set to Active.
4. Select Start from the Actions menu.
   - Note: The platform only runs data jobs from Active transformations. The Action menu indicates the number of Active data jobs that can run. For example, the menu might display Start (3 of 4).

### Rollback a data job

Use rollback to revert changes made by a normalization or transformation data job.

Role required: admin or normalizer

You can only rollback completed data jobs.

1. Navigate to Field Normalization > Data Jobs > All.
2. Select the completed data job to rollback.
   - The system displays the data normalization job record.
3. From Related Links, select Rollback.
   - The values in the Pending Values Related List are removed and the data job State indicates that it was rolled back.
Normal values

A normal value replaces similar but ambiguous field values with one standard value.

Field value variations

Records values can come from multiple sources such as:
- Automated entries made by Discovery.
- Automated entries made by importing records from external systems or files.
- Manual entries made by users.

Each of these sources may describe the same field value in several different forms. For example, the **CPU Type** field on a computer CI form might display any of the following similar values:

- **E3350 (Intel) 4.5.2234**
- **Intel Xeon 5.4.554**
- **Xeon L3350**
- **L3350**

Without normalization, these variant field values results in:
- Duplicate CPU types
- Poor search results
- Complex queries and conditions to apply business logic

Creating a normal value record solves these issues by consolidating on one standard value such as **Xeon**.

Identifying variations with aliases and rules

Each Normal value record specifies how to identify variations of a normal value using a combination of aliases and rules.

**Aliases**

Aliases are known variations of an input value that normalization converts to the normal value. Use aliases when there is a short list of variant values.

For example, you could create a normal value **Xeon** that has these aliases.

- **E3350 (Intel) 4.5.2234**
- **Intel Xeon 5.4.554**
- **Xeon L3350**
- **L3350**

Whenever a normalization data job or normalized query sees a field value matching an alias, it automatically replaces the field value with the normal value. Normalization data jobs and queries process aliases before rules.

**Note:** Aliases are logically equivalent to rules using the [is] operator in a condition where [Field name][is][Alias value]. For example, the sample aliases are equivalent to these rules: [CPU Type][is][E3350 (Intel) 4.5.2234] OR [CPU Type][is][Intel Xeon 5.4.554] OR [CPU Type][is][Xeon L3350] OR [CPU Type][is][L3350]
Rules

Rules specify the conditions under which normalization replaces an input value with the normal value. Use rules when there are a large number of possible variant values, or when you must create complex conditions.

For example, the normal value *Xeon* could have this rule.

```
[CPU Type][matches regex][.*\bxeon\b.*]
```

Whenever a normalization data job or normalized query sees a field value matching a rule, it automatically replaces the field value with the normal value. Normalization data jobs and queries process rules after aliases.

Rules and aliases can be combined to normalize a field. Make sure to test your normalization methods before applying them to all the existing records in the database.

Normalized queries

An administrator can configure normalization to apply to queries issued against normalized fields in lists. Select the **Normalize query** check box on the Normalization form to enable this functionality. In a list containing normalized values, create a filter using the original (raw) value for the normalized field in the query condition.

Normalized query example

The filtered list returns records with the normal value substituted for the raw value. However, the breadcrumbs for the filter display the original query conditions.
Scripting and normalization

Scripts that update or insert records into the database (GlideRecord) are normalized automatically when field normalization is applied. For example, if a script to insert a CI record contains a CPU type of Xeon L3350, the script is normalized to insert the CI with a CPU type of Xeon instead. Scripts that query the database for normalized field values (using the conditions of equals or not equals) can be configured to return the normal value (such as Xeon) rather than the original (raw) value.

Create the normalization record

Regardless of the normalization method selected, all field normalization requires a list of existing variants and a normal value that is configured to replace these variants in forms and in queries.

Normalize a field by selecting aliases for a normal field value or by creating rules that use condition statements to match field variants with a normal value.
Note: Users must have the normalizer role to create and manage normalization records.

Special Cases

- Reference fields cannot be normalized. To normalize values appearing in reference fields, normalize the field in the target table. Examples of this would be normalized values for the **Name** fields in the Company [core_company] and Location [cmn_location] tables, which are referenced by other tables in the platform. The normalized names are available to all fields that reference these tables.
- Fields in a choice list can be normalized if they are of a type **string**.

1. Activate the Field Normalization plugin.
2. Navigate to **Field Normalization > Configurations > Normalizations**.
3. Click **New**.
4. Create a normalization record.

### Normalization record fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Input value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name for this normalization record. This value is for reference only and is not used in any processing.</td>
</tr>
<tr>
<td>Table</td>
<td>Select the ServiceNow table for the field being normalized.</td>
</tr>
<tr>
<td>Field</td>
<td>Select the field to normalize.</td>
</tr>
<tr>
<td>Mode</td>
<td>The three available modes are Off, Test, and Active. All normalization records are created in the test mode by default. If you are planning to select aliases for your normal values, change the Mode to Active. If you intend to normalize the field using rules, be sure to leave this record in the Test mode. To disable this normalization, switch the mode to Off.</td>
</tr>
<tr>
<td>Normalize query</td>
<td>Select this check box to apply the field value normalized by this record to all queries involving this field. Queries formed with the raw (original) field value return records displaying the normal value. Queries issued by a script using the conditions equals or not equals return normalized values. See Normalized Queries for details.</td>
</tr>
<tr>
<td>Coalesce each normal</td>
<td>Select this check box to normalize reference field values. This option resets all references to records containing an alias field value to the record using the normal value. See Coalesce Normal Values for details.</td>
</tr>
</tbody>
</table>
Select the field to use to display the original (non-normalized) input values on a form in which a field value has been normalized. For the selection to appear in the drop-down list, add a custom field to the form for the table selected. For instructions on adding a field for raw data, see Creating a Raw Field.

After the normalization record is submitted, the platform runs the Pending value collection job in the Data Jobs related list automatically to gather all the current values (Pending Values) for the field being normalized.

Click the Pending Values related list to view values for the normalized field that have been entered manually, imported into the platform, or created by Discovery.
Create a normal value

A normal value is a simplified, generic value for a field that replaces all the possible variants of that value that exist in the database.

Role required: admin or normalizer

Normal values should be clear and unambiguous.

After the platform runs the data job, the Pending Values related list on the Data normalization jobs form is populated with all the unique values for the field in the database. Examine the values in the list and decide which
normalizing method is best for the existing data. For example, define an alias for a small pool of values and a rule for a large pool of values. The following screenshot shows the pending values for CPU types in Linux servers in a network. The list contains several choices for Intel Xeon CPUs, which might be normalized as Xeon.

Normalization pending values 2

1. Navigate to Field Normalization > Normalizations.
2. Open the appropriate normalization record.
3. Click the Normal Values related list.
4. Click New.
5. In the Normal Value form, create normal values for the variants in the **Pending Values** related list. These are the values the platform uses to replace the variants configured as aliases.

### Create aliases

Aliases are the variants of a field value in the instance that will be replaced by the normal value.

Role required: admin or normalizer

The list of potential aliases is the contents of the **Pending Values** related list. After creating a normal value, assign aliases to this value if the pool of pending values is small. A normalized field can have a combination of aliases and rules.

1. Navigate to **Field Normalization > Configurations > Normalizations.**
2. Open a normalization record.
3. Click the **Normal Values** related list.
4. Select one of the values.
5. In the normal value record, click the **Aliases** related link.
6. Select aliases for this normal value from the available (pending) values that appear in the slushbucket, and then click **OK**.

![Aliases for: Xeon](image)

The aliases for this normal value now appear in the **Aliases** related list.

Apply the aliases by running the associated data jobs.

**Apply aliases**

After testing, aliases can be normalized in all new records or in existing records when they are updated.

Each time an alias is created for a normal value, a data job is created. The alias is not applied to values in the entire database until its data job is started manually. Run each job separately or run the jobs together to apply all aliases at once.

1. In a normalization record, ensure that the Mode is set to **Active**.

   Data jobs cannot run in the **Test** mode.

2. Click the **Normal value** related list.

3. Select a value from list.

4. In the Normal Value record, select the **Data Jobs** related list.

   A data job is listed for each alias configured for this normal value.

5. Run the extant data jobs to replace the aliases with the normal value in all existing records in the database.

   a. Select the check box next to a job, and then select **Start** from the Actions menu.

   b. To run all data jobs at once, select all the check boxes, and then select the **Start** action.

   c. Refresh the list to check the progress of the data jobs to ensure that they complete normally.
Create rules

The use of rules to normalize a field is intended for large lists of variant field values.

Always test your rules before applying them to all the existing records in the database. Prior to creating the rule, make sure to generate the list of Pending Values and create a normal value for the field. A normalized field can have a combination of aliases and rules.

The rules in this example are based on the following Pending Values:
Normalization rules 3

1. In a Normalization record, open the **Normal Values** related list.
2. Open a Normal Value record.
3. Open the **Rules** related list in the Normal Value form, and then click **New**.

The Field Normalization Rule form provides the following fields:

<table>
<thead>
<tr>
<th>Field normalization rule fields</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Order</td>
</tr>
<tr>
<td>Active</td>
</tr>
<tr>
<td>Make alias</td>
</tr>
<tr>
<td>Case sensitive</td>
</tr>
<tr>
<td>Rule</td>
</tr>
</tbody>
</table>

4. Create a set of rules to incorporate all the possible variants of the pending values.

For this example, the rules might be:

- **Intel Xeon**: CPU type matches pattern *Intel*\(^*\)Xeon*. This rule normalizes all variants in which Intel precedes Xeon, including **Intel Xeon**, **Intel(R) Xeon(TM) CPU 2.80GHz**, and **Intel(R) Xeon(TM) CPU 3.00GHz**.
- **Xeon**: CPU type contains Xeon
- **L3350**: CPU type contains L3350
- **E3350**: CPU type contains E3350

For every rule that is created, the platform generates a **Rule applier** data job. In the testing mode, the **Start** controls are not available, and the job cannot be run until the mode is changed to **Active**.

5. Test all the rules before making the normalization record **Active**.

Testing Rules

**Note:** Users must have the normalization_tester role to create test records.

Field normalization records are created in the **Test** mode by default, enabling administrators to test normalization rules thoroughly before applying them to the existing records in the database. In the testing mode, the **Start** controls are not available for the **Rule applier** data job. The job can be run only when testing is complete and the **Mode** has been changed to **Active**. In the testing mode, only records that have been created or updated by a user with the normalization_tester role are normalized. The normalizer and normalization_tester roles can be combined for a single user or granted separately.
Coalesce records on a normal value

Coalescence enables an administrator to redirect references to multiple records containing variants of the same field value to point to a single record, based on a normal value.

An example of this is the Company table that might have multiple variants of a company name, such as Hewlett-Packard, Hewlett-Packard, Inc., Hewlett-Packard Incorporated, HP, and so on. Potentially, thousands of records might reference each of these duplicate company records. Using the variants of the Hewlett-Packard name as aliases, coalescence unifies all these references into a single record that normalizes the Name field in the Company record to a normal value such as HP.

Note: Coalescing normal values changes the record values permanently. If a rollback is performed, records will be returned to the table, but the normalized values will not be rolled back to the original variants.

1. Navigate to Field Normalization > Configuration > Normalizations
2. Select a normalization record.
3. Enable Coalesce each normal.
   The system adds the Coalesce to field to the Normal Value form.
4. Create one or more normal value records for this normalization record.
   Create related aliases and rules as needed.
5. For each normal value record, set Coalesce to by selecting the record that contains the normal value.
   For example, suppose your Company table contains several variations of the name ServiceNow. When you create the Normal Value record, you select the Company record for ServiceNow, Inc. During normalization, the system updates any references to variant records to instead refer to the normal record.
   The system updates any references to records that match aliases and rules to instead point to the normal record.
   The system also deletes the duplicate records from the table.
6. Start all the Alias application data jobs to replace the aliases with the normal value in existing records in the database.
   The system starts the Coalesce to normal data jobs for each alias.

Transforms

Transforms update field values by applying a transformation definition to the field contents such as replace text, change case, or round value.

Transform definitions

Transform definitions define the transformation actions available for a given field type. Administrators select a definition when they transform a field, and then provide the definition with the specific parameters that are applied to the transformation. For example, a definition can round up an integer or insert a value at a defined position in a string.

The system provides a number of definitions that are designed to meet the needs of most organizations, but administrators can create new definitions as needed. Transform definitions can be associated with existing Transform Categories or to new categories.

Transform categories

Transform categories are used to group the transform definitions together appropriately to present to users when creating new field transforms. You can create new categories for existing definitions or change the default associations of categories to definitions.
Transform categories are associated with normalization field types to present the correct definition option list for the field being transformed. The base system provides two transform categories: Text and Numeric.

**Text**
Definitions in the Text category transform string type field values. Included in the Text category are:

- Left
- Right
- Constant
- Trim
- Prefix
- Suffix
- Change Case
- Delete
- Insert
- Substring
- Replace

**Numeric**
Definitions in the Numeric category arithmetically manipulate integer type field values. Included in the Numeric category are:

- Limit
- Round
- Constant

**Transformation testing mode**
Transformation is a powerful tool that can cause data issues if used incautiously. Test all transformations before committing the changes to the CMDB.

All transformation records open in **Test** mode by default, which blocks administrators from running manual data jobs that apply changes to existing data. Only users with the normalization_tester role can transform data when a record is in the **Test** mode. This is limited to new records opened by the tester or records in which the transformed field is updated by the tester.

To apply transformations to the CMDB after testing, change the mode to **Active** in the transformation record and run the appropriate data job. For information on testing transforms, see Test a transform.

**Transform a field**
Transform the contents of field using a set of rules and conditions.

Role required: admin or normalizer

1. Create a transformation record.
2. Create one or more related transform records.
3. Test the transform.
4. Runs data jobs.

If you want to also show what the original (raw) input value was prior to transformation, create a raw field to store this value.
Create a transformation record
Creating a transformation record is the first step in transforming a field.

1. Activate the Field Normalization plugin.
2. Navigate to **Field Normalization > Configurations > Transformations**.
3. Click **New**.
4. Create a transformation record.

### Transformation record fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name for this transformation record. This value is for reference only and is not used in any processing.</td>
</tr>
<tr>
<td>Table</td>
<td>Select the ServiceNow table containing the field being transformed. It is important to understand the table hierarchy when setting up a field transform. For example, if you configure transformation for a field in the Computer [cmdb_ci_computer] table, that field will be transformed for all workstation machines, Windows servers, Linux servers, and UNIX servers.</td>
</tr>
<tr>
<td>Field</td>
<td>Select the field to transform. The list presented contains only those field types (integer and string) from the table selected that can be transformed.</td>
</tr>
</tbody>
</table>

**Note:** The sys_user record that initiates the transform process must have its date format set to the default format of “yyyy-MM-dd.” Any other date format causes an error during transformation. This problem is only specific to transforming TO TARGET fields of type Date/Time. This problem is not an issue if the target field type is of type String or if the field mapping for the date field is changed to the same date format as the transformation process.

<table>
<thead>
<tr>
<th>Mode</th>
<th>The three available modes are <strong>Off</strong>, <strong>Test</strong>, and <strong>Active</strong>. All transformation records are created in the test mode by default. Do not change the mode until you have thoroughly tested the transformation. When testing is complete, change the mode to <strong>Active</strong>. To disable this transformation, switch the mode to <strong>Off</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normalize query</td>
<td>Select this check box to apply the field value transformed by this record to all queries involving this field. Queries issued with the raw (original) field value will be edited to use the transformation value.</td>
</tr>
<tr>
<td>Raw field</td>
<td>Select the field to use to display the original input (non-normalized) values on a form in which a field value has been normalized. For the selection to appear in the drop-down list, add a custom field to the form for the table selected. For instructions on adding a field for raw data, see Create a raw field.</td>
</tr>
</tbody>
</table>
5. Click **Submit**.

The **Transforms** and **Data Jobs** Related Lists appear on the form.

**Create one or more related transform records**

Each related transform record performs a specific transformation type such as adding characters to the beginning of the value or replacing one string for another. You may need to create multiple related transform records to generate a preferred output field value.

1. In the Transformation record, select the **Transforms** Related List.
2. Click **New**.

A selection list of transform types appears, displaying only those transformations appropriate for the field type selected.

**Choose the type of transform you want to create:**

- **Text**
  - **Transforms that modify the text of the value.**
    - **Change Case**
      - Adjusts the case of characters in the value
    - **Constant**
      - Supply a constant value
    - **Delete**
      - Delete specified sequence of characters from the value
    - **Insert**
      - Insert a fixed character sequence into the value
    - **Left**
      - Keep or delete the leftmost 'n' characters
    - **Prefix**
      - Adds characters to the beginning of the value
    - **Replace**
      - Replaces occurrences of one string with another
    - **Right**
      - Keep or delete the rightmost 'n' characters
    - **Substring**
      - Keep or delete characters from a specified sub-sequence of characters in the value
    - **SUFFIX**
      - Append characters to the end of the value
    - **Trim**
      - Remove any leading or trailing spaces or tabs

**Transform types**

3. Select a transform type and provide the appropriate parameters.
4. Select an **Order** number for this transform.

**Note:** The conditions for the transforms are executed according to the order numbers assigned.

5. Select the **Final** check box to stop processing with this transform if the condition evaluates to true.
6. Select the **Case sensitive** check box to force case sensitivity in the condition statement.

The following transform example replaces the **INC** at the beginning of an incident number with the string **ENG** if the assignment group is **ITSM Engineering**.

![Transform Example](image)

Transformation record

7. Click **Submit**.

The new Transform appears in the Related List of the Transformation record.

When the Transform is created, a Transformation application data job is also created. This data job applies this transform to appropriate records in the entire database and should not be run until testing is complete.

8. Optional: Repeat steps 2 through 8 until the output value meets your desired criteria.

**Test a transform**

Verify the transform changes the field value as desired before applying them to existing records in the database.

- **Note:** Users must have the normalization_tester role to create test records.

New transformation records open in the **Test** mode by default, enabling administrators to test transforms thoroughly before applying them to the existing records in the database. In the test mode, the **Start** controls are not available for the Transformation application data job. There are two methods, listed below, for testing transforms before committing the transformations to existing data.

- Manually create or update test records.

In the test mode, only records that have been created or updated by a user with the normalization_tester role are transformed. Grant the normalizer and normalization_tester roles to the same user or grant them to separate users.
• Use the Test transforms utility to enter a raw value and see the resulting transformed value.

This feature enables a normalization tester to transform field values on the fly without opening or updating records. This utility tests all the transforms configured for this field.

a) Open a Transformation record.

b) Click the Test transforms Related Link.

A dialog box appears for testing field values.

c) Enter a value to transform in the Raw data field.

d) Click OK.

The platform transforms the raw value in the Transformed data field.

e) Enter new raw data to test other transforms.

f) Click Cancel to end the test.

g) When testing is complete, change the Mode to Active and run the data job.
### Default Transform Definitions

The system offers default transform definitions for fields containing text, text numeric, and numeric values.

#### Transform Definitions

<table>
<thead>
<tr>
<th>Transform Type</th>
<th>Category</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
</table>
| Change case   | Text           | Changes the case of the characters in the field value.                      | **Mode:** Select one of the following modes:  
• **Upper:** Converts the value to all upper case characters  
• **Lower:** Converts the value to all lower case characters  
• **Proper:** Converts the value to title case, with the first character in each string in upper case, and the remaining characters of the string in lower case.  
• **Formal:** Converts the value to a string in which only the first letter of the first word is in upper case. |
| Constant      | Text Numeric   | Converts the value in this field to a constant.                             | **Constant:** The constant with which to replace the value in this field. |
| Delete        | Text           | Delete a specified sequence of characters from a field value.               | **Starting position:** Specifies the first character in a sequence of characters to delete from a string. See the discussion of position modes at the beginning of this section for details.  
• **Ending position:** Specifies the final character in a sequence of characters to delete from a string. See the discussion of position modes at the beginning of this section for details. |
| Insert        | Text           | Insert a fixed character sequence into a field value.                      | **Position:** The character position at which to insert the new value. See the discussion of position modes at the beginning of this section for details.  
• **Insert:** The value to insert into this field. |
| Left          | Text           | Deletes or keeps a specified number of characters from the left side of this field value. | **Position:** Specifies the number of characters to keep or delete from the left side of the value. See the discussion of position modes at the beginning of this section for details.  
• **Mode:** Select the mode for this transform: **Keep** or **Delete**. |
<p>| Prefix        | Text           | Adds characters to the beginning of a field value.                         | <strong>Prefix:</strong> Defines the characters to add to the beginning of the transformed field value. |</p>
<table>
<thead>
<tr>
<th>Transform Type</th>
<th>Category</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
</table>
| Replace       | Text     | Replaces occurrences of one string with another string. The special characters backslash (\) and dollar sign ($) in the replacement string can cause the transform to be different than if the replacement string were being treated as a literal replacement string. Use a regular expression to replace a string or parts of a string. | • **Find**: Enter the string or regular expression to replace.  
  • **Replace with**: Enter the replacement string. |
| Right         | Text     | Retains or deletes a specified number of characters from the right side of a field value. | • **Position**: The number of characters to delete or keep from the right side of this transformed field. See the discussion of position modes at the beginning of this section for details.  
  • **Mode**: Select the mode for this transform: **Keep** or **Delete**. |
<table>
<thead>
<tr>
<th>Transform Type</th>
<th>Category</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
</table>
| Round         | Numeric  | Rounds integers to a configured rounding interval using specific criteria. The interval must be appropriate to the value being transformed, such as an interval of 12 for a value expressed in dozens or 0.01 for decimal values expressed in hundredths. | - **Interval**: Select the rounding interval that is appropriate to the units of the field value. For example, an interval of 256 is appropriate for expressing RAM values in megabytes, but does not work for Disk space expressed in gigabytes. The rounding interval for the examples below is 1. - **Mode**: Criteria for applying the rounding interval.  
  - **Half up**: Always round up a value that is exactly half way between two intervals. For example, 3.5 is always rounded up to 4, and -3.5 is always rounded up to -3.  
  - **Half down**: Always round down a value that is exactly half way between two intervals. For example, 3.5 is always rounded down to 3, and -3.5 is always rounded down to -4.  
  - **Half away from zero**: Always round an integer that is half way between the specified interval away from zero. For example, 3.5 is always rounded to 4, and -3.5 is always rounded to -4.  
  - **Half toward zero**: Always round an integer that is half way between the specified interval toward zero. For example, 3.5 is always rounded to 3, and -3.5 is always rounded to -3.  
  - **Half to even**: Always round an integer that is half way between the specified interval to the nearest interval whose least significant digit is even. For example, 3.5 is always rounded to 4, and 4.5 is always rounded to 4.  
  - **Half to odd**: Always round an integer that is half way between the specified interval to the nearest interval whose least significant digit is odd. For example, 3.5 is always rounded to 3, and 4.5 is always rounded to 5.  
  - **Up**: Always round an integer up by the specified rounding interval. For example, 3.4 is always rounded up to 4 by a rounding interval of 1.0.  
  - **Down**: Always round an integer down by the specified rounding interval. For example, 4.6 is always rounded down to 4 by a rounding interval of 1.0.  
  - **Away from zero**: Always round an integer away from zero by the specified rounding interval. For example, 3.3 is always rounded to 4, and -3.3 is always rounded to -4 by a rounding interval of 1.0.  
  - **Toward zero**: Always round an integer toward zero by the specified rounding interval. For example, 3.3 is always rounded to 3, and -3.3 is always rounded to -3. |
### Create a transform definition

The following example describes the procedure for creating a new transform definition. In this example, we create a definition that transforms a number field to an odd or even integer. The transform category is **Numeric** and the normalization field type is **Integer**.

1. Navigate to **Field Normalization > Administration > Transform Definitions**.
2. Click **New** in the record list.
3. Enter a name for this definition.
   
   **Note:** In this example, we enter **Odd/Even**.
4. Enter a brief description of the action, such as, **Transforms an integer to an odd or even value**.
   
   This information appears in the definition choice list when a user selects a new transform.
5. Right-click in the header bar and select **Save** in the context menu.

   Two Related Lists appear in the form.

   - **Transform Categories:** Click **Edit** and select **Numeric** as the category to which this definition belongs. Currently, field transformation supports two categories: **Numeric** and **Text**. The **Integer** normalization field type is already associated with this category.
   - **Transform Variables:** Define any variables required by this transform definition to perform an action on a field value. Variables are not necessary if a script can perform the action alone.

### Create a transform variable for a transform definition

Transform variables enable an administrator to apply the same definition to different fields in different ways. Transform variables contain values used by a script to perform a field transformation. Scripts and variables can be created in either order, but the script must use the transform variables. Transform variables are populated with values when a user configures a transform type.

1. In the Transform Definition record, click **New** in the **Transform Variables** Related List.

---

<table>
<thead>
<tr>
<th>Transform Type</th>
<th>Category</th>
<th>Description</th>
<th>Parameters</th>
</tr>
</thead>
</table>
| Substring     | Text       | Keep or delete characters from a specified sub-sequence of characters in the field value. | - **Starting position**: Specifies the first character in a sub-sequence of characters within the value. See the discussion of position modes at the beginning of this section for details.
|               |            |                                                                            | - **Ending position**: Specifies the final character in a sub-sequence of characters within the value. See the discussion of position modes at the beginning of this section for details.
|               |            |                                                                            | - **Mode**: Select whether to **Delete** the sub-sequence selected or **Keep** only those characters defined. |
| Suffix        | Text       | Appends characters to the end of a field value.                           | **Suffix**: Defines the suffix to add to the end of the field value.       |
| Trim          | Text Numeric| Removes blank spaces from the field value.                                | No parameters                                                              |
2. Complete the form.

   Important considerations for completing a form:
   - The Column name is an entry in the fn_transform_var table for this variable. This becomes the variable in the script, in the form of variables.<variable name>. For example, odd_even.
   - The value in the Label field appears as the variable field label in the Transform form. For example, Odd/Even.
   - The field Type defines the field type of the variable value. Because the values for the variables used are even and odd, this is a type of string.
   - The Order of the variables controls the order in which they are displayed in lists and records.
   - This variable has a choice list with two options: Even and Odd. Select Dropdown without - None as the format for the list in the Choice field and define a Default value of even when the list is displayed.
   - Create a Hint that becomes a tooltip for the variable in the Transform record.

3. Right-click in the header bar and select Save from the context menu.

   The Variables Choice List Related List appears.

4. Click New in the Variables Choice List and define the list options.

5. Create records for Even and Odd.

   Note: The Element value is the same as the Column name in both selections for the choice list.

6. Save the choice list variables and return to the transform definition form to create the script.

Create a script for a transform definition

Create the script at any time during the configuration of a definition.

The script can perform a transform action without using a variable, but the action of the definition will be the same for all fields. Variables create more flexibility for the definition, enabling an administrator to use the same definition in different ways in different places. If a variable is defined, the script must reference the variable using the correct format.

There are three arguments in the script:
   - Variables: Contains the variables using the format variables.<variable name>.
   - Value: Contains the un-transformed value
   - Parameters: Special objects that set debug messages.

All position parameters (such as Starting position and Ending position) have three modes that apply to all the transform types that use this variable.

Position parameters

<table>
<thead>
<tr>
<th>Positive positions</th>
<th>If the position is expressed as a positive integer, the platform calculates the starting position beginning from the left side of the field value. For example, in the string ABCDE, a position of 3 places the starting point of the action after C.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Negative positions</td>
<td>If the position is expressed as a negative integer, the platform calculates the position beginning from the right side of the field value. For example, in the string ABCDE, a position of -3 places the starting point of the action before C.</td>
</tr>
</tbody>
</table>
If the position value starts with /regex/, everything after that is a regular expression that is used to calculate the starting position. For example, in the string ABCDE, a position of /regex/B.*D places the starting point of the action after C (B and all the characters between B and D).

1. Open the **Odd/Even** record in the Transform Definitions module.
2. Enter the following script to pass values with the odd_even variable.

```javascript
function(variables, value, parameters) {
    var odd = ('odd' == variables.odd_even);
    var val = value - 0;
    var val_odd = ((val & 1) == 1);
    if (odd != val_odd)
        val++;
    return '' + val;
}
```
The script references the variable in the form variables.odd_even.
Transforms an integer to an odd or even value

```javascript
function(variables, value, parameters) {
    var odd = ("odd" == variables.odd_even);
    var val = value - 0;
    var val_odd = ((val & 1) == 1);
    if (odd != val_odd)
        val++;
    return "" + val;
}
```
3. Update the record to complete the configuration.
   
The Odd/Even transform definition is now ready to use in a field transformation.

Create a transform category

Create a transform category to group the transform definitions together.

1. Navigate to Field Normalization > Administration > Transform Categories.
2. Click New in the Transform Categories Related List.
3. Enter the Name of this category and a description.
4. Select an Order for this category and save the record.
   
The order determines the display order of categories in lists and forms. Two Related lists appear:
   
   • Field Types: Click Edit to select an existing field type for this category or click New to create a new field type. The normalization field types provided are:
     • Decimal
     • Float
     • Integer
     • Numeric
     • String
     • URL
   
   • Transform Definitions: Click Edit to select the transform definitions that are included in this category.

Regular expressions and patterns in field normalization rules

Field Transformation definitions support the use of regular expressions (referred to in the platform as regex) and pattern matching for determining the position of characters in a string.

After identifying the target characters, field transformation can replace or delete the identified characters or insert other characters at that position.

Regex

Regular expressions can be used in transform parameters and in condition statements to determine which characters in a field value are transformed.

   • Transform parameters: Regular expressions used as parameters to locate characters in transformed field values must begin with /regex/. Everything after that is a regular expression that is used to calculate character position.

Example

The computer names in an organization's Windows network are expressed as domain\machine name, such as development\devlab01. The network administrator wants to simplify these names by removing the domain name and backslash. He creates a transformation record for the Computer [cmdb_ci_computer] table and selects the Name field to transform.
The network contains several domains, and each domain contains numerous computers. The only character common to each name is the backslash. To delete the domain name, the administrator decides to use a regular expression to replace the entire raw value in the field with the characters that appear after the backslash (the actual machine name). He creates a new Transform using Replace as the Transform Type and enters the following values:

- Find:/regex/.*/\((.*)
- Replace with:$1

Transformation regex example
The regular expression \\.*\(.*\) represents the entire raw value in the Name field - in this example development \devlab01. The first part of the expression, .*, represents everything before the backslash (the development domain name). The backslash by itself is the escape character in regular expressions and requires special syntax to retain its function in the computer name. The administrator must escape it by using another backslash (\ means \). The part of the expression after the backslash, (.*), represents the computer name (devlab01) and is grouped within parentheses for reference. The value in the Replace with field, $1, references this group and replaces the entire raw value of the field with the contents of the group, devlab01.

The administrator clicks Test transforms in the transformation record and enters development\devlab01 in the Raw data field. He then clicks OK to apply the transform to the test value. The transform replaces development\devlab01 with devlab01.

When the transforms for this field are tested successfully, the administrator changes the Mode in the transformation record to Active and runs the Transformation application data job to apply this transformation to existing records in the database.

Pattern matching

Pattern matching in Field Normalization uses special characters differently from regular expressions to create patterns that the platform recognizes when transforming field values.

Pattern matching can be used only in condition statements. When using pattern matching characters in a condition statement, make sure to select the matches pattern operator.

Use the following special characters to create patterns for searches.

- The asterisk in a search string (*) matches any number (including zero) of any character.
- The question mark (?) in a search string matches one of any character.
- Everything else in a search string matches itself.

Examples

- the story matches the story but not that story.
- *story matches the story and that story, but not that story is the best.
- st?ry matches story and stxry, but not my story or stairy.
- *b?gus* matches bogus, my bogus story, and His bagus machine, but not my bgus story or my baigus story.
Domain separation and Field Normalization

Domain separation is unsupported in Field Normalization. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can control several aspects of this separation, including which users can see and access data.

Support level: No support

- The domain field may exist on data tables but there is no business logic to manage the data.
- This level is not considered domain-separated.

For more information, see Application support for domain separation.

Data policy

Data policies enable you to enforce data consistency by setting mandatory and read-only states for fields.

Data policies are similar to UI policies, but UI policies only apply to data entered on a form through the standard browser. Data policies can apply rules to all data entered into the system, including data brought in through import sets or web services and data entered through the mobile UI.

For example, suppose that you are configuring a web service that allows users from outside the platform to update problems on the ServiceNow instance. Since these problems are not updated through the instance UI, they are not subject to the UI policies on the problem form. To ensure that the Close notes field is completed before a problem is marked Closed/Resolved, you can create a data policy that applies to server-side imports. Data that does not comply with this data policy produces an error. You can also apply the policy on the browser by selecting the Use as UI Policy on client check box in the data policy record.

Since UI policies can also manage the visibility of fields on a form, you may want to augment UI policies with data policies rather than replace them.

By default, data policies are applied to all GlideRecord operations including those used in Scripted REST APIs, and the REST Table API. You can opt out of applying the data policy to:

- Target records of SOAP web services
- Import sets
- Client-side UI policies

The admin role is required to edit data policies.

Note: Defining a data policy enforces the policy when a record is submitted from the UI. This behavior cannot be changed.

Installed with data policy

Data policy includes several components that are installed on the instance.

Tables

- Data Policy [sys_data_policy2]
- Data Policy Rule [sys_data_policy_rule]

Roles

The following role is available with data policy:
data_policy_admin: Allows you to grant access for maintaining data policy to specific users. You may have to grant this role access to the System Policy application.

Data Policy Module

The **System Policy > Data Policies** module displays a list of all data policies and where they apply.

**Create a data policy**

You can create a new data policy to define data rules for a table.

Create data policies to enforce consistency. You can create data policies only for tables and database views that are in the same scope as the data policy and for other tables that have at least one field in the same scope as the data policy. For tables that are in a different scope from the data policy record, you can create data policy rules only for fields in the same scope as the data policy and you cannot make a field mandatory.

1. Navigate to **Data Policies** by completing one of the following actions.
   - Navigate to **System Policy > Rules > Data Policies**.
   - From any form header, right-click the header bar and select **Configure > Data Policies**.
   - In List v2, open any column context menu and select **Configure > Data Policies**.
   - In List v3, open the list title menu and select **Configure > Data Policies**.
2. Click **New**.
3. Select any options for the data policy.
4. Create the condition that must exist for the platform to apply this policy.
   - For example, your conditions might include `[Problem state] is [Closed/Resolved]`
5. Right-click the header and select **Save**.
   - The **Data Policy Rules** related list appears.
6. Click **New** in the related list and create the record that identifies the field and the policy to apply.

It is possible to have multiple rules on a single field, but it is not recommended.
7. Click **Submit**.
8. Optional: Add more rules by repeating steps 6 and 7.

### Data policy fields

These fields appear on the Data Policy form and related forms.

#### Data policy fields

<table>
<thead>
<tr>
<th><strong>Field</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>The table to which this policy applies.</td>
</tr>
<tr>
<td><strong>Note:</strong> The list shows only tables and database views that are in the same scope as the data policy.</td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>Application that contains this data policy.</td>
</tr>
<tr>
<td>Inherit</td>
<td>If selected, applies this data policy to tables that extend the specified table. For example, incident, problem, and change tables all extend the task table, therefore selecting Inherit on a data policy defined for task would apply the data policy to them as well.</td>
</tr>
<tr>
<td>Reverse if false</td>
<td>If selected, the data policy action is reversed when the conditions evaluate to false. For example, when the conditions are true, then actions are taken and when they change to false, the actions are reversed.</td>
</tr>
<tr>
<td>Active</td>
<td>If selected, the data policy is used.</td>
</tr>
<tr>
<td>Short description</td>
<td>A short description that identifies the policy.</td>
</tr>
<tr>
<td>Description</td>
<td>A detailed description of the policy.</td>
</tr>
<tr>
<td>Apply to import sets</td>
<td>If selected, the data policy applies to data brought into the system from import sets. This option also applies to web service import sets.</td>
</tr>
<tr>
<td>Apply to SOAP</td>
<td>If selected, the data policy applies to data brought into the system from a SOAP web service. Scripted SOAP web services are not affected. This field does not affect data policy interaction with REST web services.</td>
</tr>
<tr>
<td>Use as UI Policy on client</td>
<td>If selected, enforces the data policy on the UI using the UI policy engine.</td>
</tr>
</tbody>
</table>

#### Data policy rule fields

<table>
<thead>
<tr>
<th><strong>Field</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>The table on which the data policy action applies.</td>
</tr>
<tr>
<td>Field name</td>
<td>The field from the specified table to which the data policy will apply.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Read Only</td>
<td>How the data policy affects the read only state of the field. Choices are:</td>
</tr>
<tr>
<td></td>
<td>• Leave alone</td>
</tr>
<tr>
<td></td>
<td>• True</td>
</tr>
<tr>
<td></td>
<td>• False</td>
</tr>
<tr>
<td>Mandatory</td>
<td>How the data policy affects the mandatory state of the field. Choices are:</td>
</tr>
<tr>
<td></td>
<td>• Leave alone</td>
</tr>
<tr>
<td></td>
<td>• True</td>
</tr>
<tr>
<td></td>
<td>• False</td>
</tr>
</tbody>
</table>

**Note:** For tables that are in a different scope than the data policy record, you cannot make a field mandatory.

**Convert a UI policy to a data policy**

To make a UI policy the default setting, convert the UI policy to a data policy.

Role required: ui_policy_admin

You can also apply a UI policy to import sets or to data imported by SOAP web services when you convert it to a data policy. Converting a UI policy to a data policy deactivates the UI policy. To retain the policy in the UI, ensure that the **Use as UI Policy on client** check box is selected on the data policy record.

For a UI policy to be eligible for conversion to a data policy, the following conditions must be met on the UI Policy form.

- The **Run scripts** check box must be cleared.
- The **Global** check box must be selected.
- None of the UI policy actions can have **Visible** set to **True** or set to **False**. **Visible** must be set to **Leave Alone**.

1. Navigate to **System UI > UI Policies**.
2. Open an existing UI policy.
3. Under **Related Links**, click **Convert this to Data Policy**.
   
   A new data policy record is created.
4. Edit the fields on the data policy record as necessary.

**Convert a data policy to a UI policy**

Converting a data policy to a UI policy is useful if a data policy already exists, but only needs to apply to records created or updated in the browser.

Role required: admin

Converting deactivates the data policy - the new UI policy is applied only at the UI layer only and not to import sets or data imported from SOAP web services.
Note: An alternative to converting from a data policy to a UI policy is to select the Use as UI Policy on client checkbox on the data policy record. This field extends the data policy to the UI. The main difference between converting and using the Use as UI Policy on client checkbox is that converting provides the Visible field on the UI policy record. Use the Visible field to select how the UI policy affects the visible state of the field.

2. Under Related Links, click Convert this to UI Policy.

A new UI policy record appears.

3. Edit the fields on the UI policy record as necessary. For details about the fields, see Create a UI Policy.

Data policy debugging

Debug messages can help administrators identify and resolve data policy problems. Debug messages can help you identify and resolve data policy problems. To view data policy debugging messages at the bottom of the screen, navigate to System Diagnostics > Session Debug > Debug Data Policies.
In the example, a data policy is in place to prevent the short description on an incident from being changed when the incident state is set to Open. A user edited the short description while the incident was open and tried to save the changes, but the data policy was enforced.

**Debug Output**

<table>
<thead>
<tr>
<th>Time</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>16:13:37.693</td>
<td>DataPolicies Found : 2</td>
</tr>
<tr>
<td>16:13:37.693</td>
<td>Running Data Policy on incident &quot;Users cannot edit the short description for a new incident&quot;</td>
</tr>
<tr>
<td>16:13:37.694</td>
<td>Evaluating Condition</td>
</tr>
<tr>
<td>16:13:37.696</td>
<td>incident_state=1*EQ - true</td>
</tr>
<tr>
<td>16:13:37.697</td>
<td>Field Short description is Read Only</td>
</tr>
<tr>
<td>16:13:37.697</td>
<td>Evaluating Condition</td>
</tr>
</tbody>
</table>

**Data policy debug messages**

**Data lookup and record matching support**

The data lookup and record matching feature enables administrators to define rules that automatically set one or more field values when certain conditions are met.

Data lookup rules allow administrators to specify the conditions and fields where they want data lookups to occur. For example, on Incident forms, there are priority lookup rules for the sample data that automatically set the incident **Priority** based on the incident **Impact** and **Urgency** values.

**Note:** Activating the Data Lookup and Record Matching Support plugin replaces the `calculatePriority` business rule with a priority data lookup definition, but does not transfer any custom logic. If you manually activate the plugin, you must recreate any custom business logic that uses the priority lookup rules.

**Create custom data lookups**

Creating custom data lookups involves adding a lookup value, creating the definition, and activating data lookup.

**Create a custom data lookup table**

Create a custom table to store lookup data.

The custom table must extend the Data Lookup Matcher Rules `[dl_matcher]` table. For example, this custom lookup table stores information about VIP callers and incident assignments.

**Custom data lookup table**

<table>
<thead>
<tr>
<th>Field</th>
<th>Sample value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>VIP Caller Lookup</td>
</tr>
<tr>
<td>Table name</td>
<td><code>u_vip_caller_lookup</code></td>
</tr>
</tbody>
</table>
Add a data lookup value to the data lookup table

The columns of a data lookup table contain both matcher and setter field data.

Each data lookup is a query that searches for a row containing values that match the matcher fields. The data lookup then returns the value listed in the setter fields. For example, this Priority Data Lookup [dl_u_priority] table lists the combinations of impact and urgency (matcher fields) that produce a particular priority value (setter field).

Lookup table

<table>
<thead>
<tr>
<th>Matcher fields</th>
<th>Setter field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact</td>
<td>Priority</td>
</tr>
<tr>
<td>1 - High</td>
<td>1 - Critical</td>
</tr>
<tr>
<td>1 - High</td>
<td>2 - High</td>
</tr>
<tr>
<td>1 - High</td>
<td>3 - Moderate</td>
</tr>
<tr>
<td>2 - Medium</td>
<td>1 - High</td>
</tr>
<tr>
<td>2 - Medium</td>
<td>2 - Medium</td>
</tr>
<tr>
<td>2 - Medium</td>
<td>3 - Low</td>
</tr>
<tr>
<td>3 - Low</td>
<td>1 - High</td>
</tr>
<tr>
<td>3 - Low</td>
<td>2 - Medium</td>
</tr>
<tr>
<td>3 - Low</td>
<td>3 - Low</td>
</tr>
</tbody>
</table>

1. In the navigation filter, enter the name of the new custom lookup table. For example, enter `u_vip_caller_lookup.list`.
2. Configure the list and create new fields, as appropriate. For this example, create the following new fields:

New fields

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Field length or Table to reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caller</td>
<td>Reference</td>
<td>User [sys_user]</td>
</tr>
<tr>
<td>Priority</td>
<td>Integer</td>
<td></td>
</tr>
<tr>
<td>Assignment Group</td>
<td>Reference</td>
<td>Group [sys_user_group]</td>
</tr>
</tbody>
</table>

3. From the table list, click New and enter appropriate matcher and setter field values. For example:

New matcher and setter field values

<table>
<thead>
<tr>
<th>Matcher field</th>
<th>Setter fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caller</td>
<td>Priority</td>
</tr>
<tr>
<td></td>
<td>Assignment Group</td>
</tr>
</tbody>
</table>
Create a data lookup definition record

Data lookup requires a definition record that specifies how to set one or more field values when specified conditions are met.

2. Click New.
3. Click Data Lookup Rule.
4. Complete the Data Lookup Rule form using the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique name to identify the definition record.</td>
</tr>
<tr>
<td>Source Table</td>
<td>Select the table containing the fields you want to automatically update with lookup values. Data Lookup Definitions are not inherited by extension tables. For example, a Data Lookup Definition on the Task table cannot match values on the Incident incident table.</td>
</tr>
<tr>
<td>Matcher Table</td>
<td>Select the table containing the lookup values. This table should always start with a u_ prefix.</td>
</tr>
<tr>
<td>Active</td>
<td>Select this check box to run this data lookup rule. Clear the check box to ignore this data lookup rule.</td>
</tr>
<tr>
<td>Run on form change</td>
<td>Select this check box to automatically look up values whenever a user or onChange client script changes a field value on a source table form.</td>
</tr>
</tbody>
</table>

**Note:** This does not include changes automatically made by other data lookup rules, such as the Priority Lookup Rules.
5. Right-click the form header and click **Save**.
6. From the **Matcher Field Definitions** related list, click **New**.
7. Complete the Matcher Field Definitions using the following table.

   A data lookup only occurs on fields with matcher field definitions. The data lookup uses the values of the source table fields to look up one or more values from the matcher table. Note that data lookup does not work with **Journal** type fields.

   **Matcher field definitions fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Lookup</td>
<td>Displays the name of the parent data lookup definition record.</td>
</tr>
<tr>
<td>Source table field</td>
<td>Select the field from the source table that contains the data to match.</td>
</tr>
<tr>
<td>Matcher table field</td>
<td>Select the field from the matcher table that contains the data to match.</td>
</tr>
<tr>
<td>Exact lookup match</td>
<td>Select this check box to require the matcher table to contain a matching row for every possible combination of values (including blank values). Clearing this check box means that any blank values in the matcher table match any value. For example, suppose the Priority field is blank in the matcher table. When this check box is selected, there is a match only when the Priority value is blank in the source table row. When this check box is cleared, the blank matcher field value matches any value in the source table field.</td>
</tr>
</tbody>
</table>

   **Note:** If the lookup does not require an exact match, matcher table rows containing blank values are treated as wild cards, matching all values.

8. Click **Submit**.
9. From the **Setter Field Definitions** related list, click **New**.
10. Complete the Setter Field Definitions form using the following table.

   **Setter field definitions fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Lookup</td>
<td>Displays the name of the parent data lookup definitions record.</td>
</tr>
<tr>
<td>Source table field</td>
<td>Select the field from the source table that the data lookup updates.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Matcher table field</td>
<td>Select the field from the matcher table that provides the new value for the update.</td>
</tr>
<tr>
<td>Always replace</td>
<td>Select this check box to replace any existing value with a value from the data lookup. Clear this check box to ignore the update if the field has an existing value.</td>
</tr>
</tbody>
</table>

11. Click **Submit**.
12. Click **Update**.

For example, the following data lookup definition assigns incidents to the VIP Issues group based on the **Caller** field. In addition, the incidents are set to critical or high priority based on the caller.

Create a data lookup module

You can create a module for data lookup so it appears in the instance application navigator.

1. Navigate to **System Definition** > **Application Menus**, then select an application to add the module to.
2. In the Modules related list, click **New**.
3. Configure a module for the data lookup table you created using the following properties.
## Module properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Required value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>Select the data lookup table you created in Step 2. For example <code>u_vip_caller_lookup</code>.</td>
</tr>
<tr>
<td>Link type</td>
<td>List of Records</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

**Troubleshooting data lookup**

If the custom data lookup definition rules are not behaving as expected, check for certain conditions.

- Verify that the data lookup definition is set to run on the appropriate events.
- Verify that the matcher field is not read-only. Since users cannot change read-only fields, user interactions cannot trigger an on form change event for read-only fields.
- Verify a client script is not changing a field value. Client scripts can trigger **Run on form change** events even on read-only fields.
- Verify that the data in the matcher table is correct.
- If the lookup requires an exact match, verify that there is a matcher table row for each possible combination (including blank values). The lookup fails if cannot find a matching value.
- Verify that you have not created a recursive rule, such as:
  - If Field A = 1, then Field B = 2. If Field B = 2, then Field A = 2

## State Management

State Management enables an administrator to define State Models and State Transitions that control how a record is allowed to transition through a predefined list of states.

An example of a state transition is when the **State** field in a facilities request is moved from the **Assigned** state to the **Work In Progress** state.

State Management is active for all instances.

### What is a state model?

A state model is a list of states that describe an expected record workflow through the lifecycle of the record. State models can be defined for any table that extends the task table. State models simplify defining the state transitions allowed for a specific task type.

In the State Model [sys_state_model] table, define the name of the state model and which task table the state model is applied to. Use the condition builder to specify any conditions for applying the state model to records and any required condition for moving between states.

For example, you could define a state model for a new custom application for airline reservations. The custom application has a Reservation Request [reservation_request] table with 4 states: **Held**, **Confirmed**, **Completed**, and **Canceled**. You could define the state model to target the Reservation Request table, and then define the state transitions for each of the 4 states. When you enable the state model, the choice list for the **State** field includes only the choices allowed by the conditions in the state transitions.

**Note:** State Management includes example state models that are copies of the normal, emergency, and standard change request state models. By default, these examples are not enabled. Use them only as examples.
to develop a state model and transitions for a task table that does not have a state model. Do not enable these example state models for change requests and then make changes to them. Doing so breaks existing transitions for change requests.

What is a state transition?

State transitions are a list of conditions for entering or exiting each state defined for a table. In the State Transitions [sys_state_transitions] table, use the condition builder to build a list of conditions required for entering or exiting each state.

To prevent users from choosing an invalid state, any attempt to update a record’s state is denied if it violates the state transitions, whether the attempt is through user input, a script, a Web API such as REST or SOAP, or any other source.

State transitions control the choice list for the State field on the target task table and prevent you from choosing any state value that does not adhere to the underlying process or does not meet the defined conditions for the transition.

For example, if the enter condition for the Completed state is State is Confirmed, only records in the Confirmed state can transition to the Complete state. When a record is in the Confirmed state, the only choice in the State field choice list is Completed.

Add a state model and transitions

Add a state model and transitions to specify conditions for moving between states.

Role required: state_model_admin or admin

Develop and test your state model in a non-production instance before deploying it in the production instance.

1. Navigate to State Management > State Models.
2. Click New.
3. Fill in the fields on the form.

State model fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Descriptive name for this state model.</td>
</tr>
<tr>
<td>Table</td>
<td>Table this state model applies to.</td>
</tr>
<tr>
<td>Application</td>
<td>Defaults to Global.</td>
</tr>
<tr>
<td>Order</td>
<td>Order in which this state model is evaluated for the target table. State models are evaluated in numerical order, from the lowest number to the highest number. Leave space between the numbers so that you can insert a new state model later, if necessary. For example, enter 10 for the first state model to be evaluated, 20 for the next state model to be evaluated, and so on.</td>
</tr>
<tr>
<td>Active</td>
<td>Indicates that this state model is enabled. Clear this check box until you define the state transitions for the state model.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of this state model.</td>
</tr>
</tbody>
</table>
Field | Description
--- | ---
Condition | Condition builder that sets the conditions for applying this state model to records. For example, you could add the condition **Category is Networking** versus **Category is Security** if there are different state models for networking requests and security requests.

Common Exit Condition | Condition builder that sets any common condition required for moving from one state to another.

4. Open the form context menu and click **Save**. The **State Transitions** related list appears.
5. Click **New** on the **State transitions** related list.
6. Fill in the fields on the form.

**State transition fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State Model</td>
<td>State model that uses this state transition.</td>
</tr>
<tr>
<td>State</td>
<td>State this transition controls, for example <strong>Ready</strong> or <strong>In Progress</strong>.</td>
</tr>
<tr>
<td>Application</td>
<td>Defaults to <strong>Global</strong>.</td>
</tr>
<tr>
<td>Order</td>
<td>Order in which this state transition is evaluated. State transitions are evaluated in numerical order, from the lowest number to the highest number. For example, if the first predefined state is <strong>New</strong>, give that state the lowest order number so that the conditions for entering and leaving the state are evaluated first. Leave space between the numbers so that you can insert a new state transition later, if necessary. For example, enter 10 for the first state transition to be evaluated, 20 for the next state transition to be evaluated, and so on.</td>
</tr>
<tr>
<td>Terminal State</td>
<td>Selected if there are no transitions from this state.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of this state transition. For example, the Description for the Assess state could be <strong>New state can move only to Assess state.</strong></td>
</tr>
<tr>
<td>Enter Condition</td>
<td>Condition builder that sets the conditions for entering this state.</td>
</tr>
<tr>
<td>Exit Condition</td>
<td>Condition builder that sets the conditions for exiting this state.</td>
</tr>
</tbody>
</table>

7. Click **Submit**. The state model form reopens, and the new transition is added to the related list.
8. Continue adding state transitions for the remaining states.
9. When finished adding state transitions in the state model form, select the **Active** check box and click **Update**.
Implement process flow and UI actions with a state model

You can implement a process flow and UI actions with a state model.

Role required: state_model_admin or admin

State models provide a way to limit the choices for moving between states in a form. If you set up only a state model, users manually change states in the form. Additional steps are required to add the process flow or UI actions, as illustrated in the following example.

1. Verify choices for the State field for the table and ensure that you created transitions for them. For more information about how to add State field choices, see Best practices for state field choice values.
2. After creating the state model, define the process flow. For more information about process flows, see Process flow formatter.
3. Define UI actions as desired to move between states. For more information about UI actions, see UI actions.

After the state model is enabled, only the defined state transitions are included in the choice list for the State field, and the process flow and UI actions are implemented.

Installed with State Model

Several types of components are installed with the State Model.

Tables installed with State Model

State Model adds the following tables.

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State Model</td>
<td>Defines the name of the state model and which table the state model targets. Also defines the condition for applying the state model to records and any common condition for moving from any state to any other state.</td>
</tr>
<tr>
<td>[sys_state_model]</td>
<td></td>
</tr>
<tr>
<td>State Model</td>
<td>Defines how each record in the target table transitions to (the enter condition) and/or from (the exit condition) each state predefined for that table.</td>
</tr>
<tr>
<td>[sys_state_model]</td>
<td></td>
</tr>
</tbody>
</table>
Roles installed with State Model

State Model adds the following role.

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
<th>Contains roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>State Model Administrator</td>
<td>Allows users to add, modify, and delete state models for task tables.</td>
<td>• None</td>
</tr>
</tbody>
</table>

Script includes installed with State Model

State Model adds the following script include.

<table>
<thead>
<tr>
<th>Script include</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TableChoiceUtils</td>
<td>Utility class to get the choice list of a table field.</td>
</tr>
</tbody>
</table>

Client scripts installed with State Model

State Model adds the following client script.

<table>
<thead>
<tr>
<th>Client script</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Populate State Choices</td>
<td>State Transition [sys_state_transition]</td>
<td>Populates the State field choices in the targeted record.</td>
</tr>
</tbody>
</table>

Business rules installed with State Model

State Model adds the following business rules.

<table>
<thead>
<tr>
<th>Business rule</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the display value for state</td>
<td>State Transition [sys_state_transition]</td>
<td>Sets the State field value based on the state model for the table.</td>
</tr>
<tr>
<td>Set the table to pick choices</td>
<td>State Transition [sys_state_transition]</td>
<td>Caches the State field value from the first table in the hierarchy for further rule processing.</td>
</tr>
</tbody>
</table>

Currency administration

Currency fields provide features for handling the calculation, conversion, and display of currency values.

The Now Platform® supports two types of currency fields:

**Default (standard) currency**

The default, or standard, currency fields that are delivered with the Now Platform.

**FX Currency**
FX Currency is an alternate type of currency field that is highly configurable, supports custom rate tables, and provides for improved visibility into conversion calculations. You can add FX Currency fields to base and custom applications, and they work independently of existing standard currency fields.

**Setting up and operating standard currency fields**

The standard, or default, currency fields are installed with the base system and used in most non-financial applications.

A standard currency field stores a currency value, a currency code, and a reference currency value.

- Three-letter ISO code that identifies the currency that you select for the currency amount. For example, USD for the US Dollar, or EUR for the Euro.
- The reference currency value is the currency value, expressed in the reference currency. When you save a currency value, the reference currency value is calculated using a rate conversion.

A price field is similar to a currency field, but with special features for conversion and display. To learn more, see Price fields.

**Locale settings**

There are two locale settings, system and user. The system locale determines the reference currency, and the user locale determines the session currency.

**System locale**

You set the system locale using the `glide.system.locale` property. The value is in the format Language.Country, where the:

- **Language** is an ISO 639 language code.
- **Country** is an ISO 3166 language code.

Internally, this value is used as specified by Java. The system locale setting should be in the Java supported locales list. Set the system locale once after a fresh zBoot, because reference currency values that appear in currency fields are in the currency implied by the system locale. To set this property, see Control default currency field configuration and use in an instance.

**Note:** Do not change the system locale after currency values have been entered into the instance. When you change the system locale, the reference currency values are not adjusted. There is no rate conversion. This persistence results in invalid aggregations and filtering.

**User locale**

The Now Platform® determines the user locale in the following sequence:

- User record in which the country, or both the country and language, are specified.
- System locale set using the `glide.system.locale` property.
- Browser locale.

Amounts in currency fields are composed of a currency code and amount. Amounts always appear in the session currency, and are formatted in the Java-specified format for the user locale.
Session and reference currency

The default, or standard, currency fields in the Now Platform® use two kinds of currency, Session and Reference.

Session currency

The session currency is defined for the user by the user’s locale or single-currency mode.

Reference

The system local determines the reference currency, and is the standard used across the entire instance.

Each time you enter a value into a currency or price field, the system stores three pieces of information:

- Value as entered, in the user's locale.
- Currency code, in the user's locale.
- Value converted to the reference currency using the current exchange rate.

Note: In multiple-currency mode, the currency code saved in the currency field may not be the same as the session currency code. For example, the session currency could be the Euro and the number entered could be the Japanese Yen.

Session currency

When users view a currency value, they can see the value as entered or in the session-currency format. The format contains the:

- Currency symbol
- Value converted to the session currency and shown in a localized number format.

The user's locale determines the session currency format.

The number format can differ in features such as the decimal separator based on the locale. For example, the US formatting is 1,234,567.89, while German formatting is 1.234.567,89. The Now Platform® determines the session currency in the following sequence:

- Single-currency mode setup using glide.i18n.single_currency and glide.i18n.single_currency.code.
- Default currency for the user’s locale.

Reference currency

To perform calculations on heterogeneous currency values, the Now Platform® stores currency values converted to a system currency, referred to as the reference currency. Every currency field contains a reference currency value. The system determines the reference currency in the following sequence:

- System locale set using the property glide.system.locale
- Java default locale, typically en.US

The filtering and aggregation features use the reference currency value to perform calculations on default currency fields. These features can yield inaccurate results because of conversion rate changes.
Issues with currency fields

Users are often confused by the results of filtering, sorting, and displaying currency fields because the system works with at least two currencies for each value: the session currency and the reference currency.

**Note:** Aggregations and filtering of currency fields use the reference currency, and the user sees the session currency. Because of changing conversion rates, the filtered reference currency values might not result in the same order as the session currency values would suggest. The same issue happens with aggregations.

The user might see the following issues:

- Lists filtered on currency fields might not be in the expected order. It uses the reference currency values for filtering but displays session currency values.
- Aggregation of currency fields may not produce the expected results because reference currency values are aggregated, and then converted to the session currency.
- Currency values may not appear as expected because currency values are formatted based on the user's locale and not on the currency code.

This confusion may be the result of the difference between session and reference currencies, changing conversion rates, and different session currencies used by different users.

Single-currency mode

Single-currency mode enables all users of the platform to view currency values in the same currency.

Before enabling single-currency mode, set the system locale. To configure single-currency mode, set the following properties:

- `glide.i18n.single_currency`: true or false
- `glide.i18n.single_currency.code`: the three-letter ISO currency code
- `glide.system.locale`: the system locale

**Note:** For detailed information about valid locale formats, see Locale settings.

Using the single-currency mode has the following limitations:

- The single-currency mode changes the currency that appears in the user views, but does not change the number formatting. Even though users in different countries see currency values in one currency, the number formatting, as determined by the user’s locale, might not be what they expect.
- Because currency value input is constrained to the single currency, price fields cannot be used.

You can avoid the effects of rate conversions by setting the system locale and the reference currency to be the single currency.

Price fields

A price field is a currency field that enables control over conversions and display. The Service Catalog uses price fields.

You can select conversion and display options per price field, and change them at any time. There are three variations:

**Calculated [Default]**
Behaves in the same way as the default currency field type. Whenever conversions are performed, it uses the latest currency conversion rates. The price field appears in the session currency for the user.

**Fixed**

When the price field appears, it is shown in the currency code used when you entered the value. Whenever conversions are performed, it uses the latest currency conversion rates.

**Multiple**

Enables you to enter multiple price values for an item using a different currency for each price. The field value is the value entered in the user’s session currency. Otherwise, the first price entered converts to the user’s session currency. Whenever conversions are performed, it uses the latest currency rates.

ℹ️ **Note:** The first value entered is used during display. The additional values are not used during calculations.

For examples of using price field, refer to the tables used in Service Catalog.

You can change the currency code and numeric value for a price field. When you click the Edit icon that appears next to the price field, a form appears that you use to edit the details for the price field:

**Price field currency details**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Currency</td>
<td>List of currencies enabled in the system in the combo box. In single currency mode, the currency is a label and cannot be changed.</td>
</tr>
<tr>
<td>Amount</td>
<td>Numeric value formatted in the user’s locale.</td>
</tr>
</tbody>
</table>
| Type    | Calculated, Fixed, Multiple.  
  - When you change the price type to Multiple, the system creates child records for all currencies enabled in the platform. The child records are populated with values converted from the amount field, using latest currency conversion rates.  
  - You cannot change the price type in single currency mode.  
  - You can modify the price type at any time. |

**Default currency values in forms**

In forms, currency values appear in the currency in which they were entered.

A combo box provides a list of available currencies, and the user’s locale determines its format. When entering or changing the numeric currency value, enter it in the same format specified by the user’s locale. In the form for a new record, the reference currency is pre-selected in the currency list, with the numeric value set to zero

- If the record is read only, the currency value appears in the Currency field as it was entered, and is formatted in the user’s locale. In the Price field, the session currency value appears.
• In Single currency mode, the currency is a label that cannot be changed, and the **Edit** icon does not appear.

**Editing the currency instance record**

If a currency instance record exists, an **Edit** icon appears next to the **Currency** field if you have edit rights for the fx_currency_instance table. Users with the financial_mgmt_user role can edit the values associated with the currency field.

**Note:** Normally, you should not edit the fx_currency_instance table directly. The Now Platform maintains these tables, and your changes could have unintended consequences.

**Default currency values in reports**

Currency values in reports appear in the user’s session currency, and are formatted in the user’s locale with a currency symbol.

The user determines how the report is run.

• Shared report: The user who runs the report.
• Scheduled report: Generally run as the user who scheduled the report.

The two user-specific values in the report are:

• User session currency
• Converted value

**Note:** A user that has a different session currency than the person who runs a report might receive unexpected results.

**Default currency values in lists**

In lists, default currency values appear in the user’s session currency, formatted for display in the user’s locale. Typically, a formatted number follows the currency symbol.

Different field types appear as follows in lists:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Currency field type</td>
<td>Value expressed in the user’s session currency.</td>
</tr>
<tr>
<td>Price field type</td>
<td>• <strong>Calculated:</strong> Value in the user’s session currency.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Fixed:</strong> Currency value, as entered by the user.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Multiple:</strong> Value associated with the user’s session currency if this value exists. Otherwise, the first value entered converts to the user’s session currency.</td>
</tr>
</tbody>
</table>

A Globe icon appears beside the currency value that enables you change to one of the following values:

• Value as entered by the user.
• Value in session currency.
• Value as entered and, in brackets, the value in reference currency.
The icon appears when the user’s session currency is different from the currency entered. Clicking the icon cycles through the listed displays. In the preview for the record, currency values appear as entered, formatted in the user’s locale.

**Aggregation**

Aggregation operations can be used on currency columns. Aggregation operations include total, group by, average, minimum, and maximum. Aggregation is done in two steps:

- Aggregate the reference currency values for all records.
- Convert this aggregate to the user’s session currency for display.

**Note:** The resulting value may not be what you expect. The conversion rate used for the value that appears for the currency field, and for its reference currency, that is used for the aggregation, may have changed.

This limitation extends to different price types.

- For price type fixed, the calculated reference value can be old.
- For price type multiple, the reference value of the first price entered is used. The other values are not used.

The aggregate value is shown formatted in user’s locale with a currency symbol. Currency fields are stored with four decimal places, and aggregates have four decimal places. For upgrades, you must set the `glide.currency_price.use_all_fraction_digits` property. See Change default currency decimal places for more information.

**Filtering**

You can set up filters on currency fields. The currency value is entered as a currency code and numeric value. Filtering is done in two steps:

- The filter currency value is converted to the reference currency.
- The filter’s calculated reference value is compared with the reference value in the records.

Matching records are shown in the list view.

**Note:** At times, the filtering results might not provide the expected result. The conversion rate used when you run the filter might be different than the conversion rate used when calculating the reference values in the individual records. This limitation extends to the following price types:

- For a Fixed price field type, the calculated reference value can be old.
- For a Multiple price field type, it uses the reference value of the first price, and does not use the other values.
Default currency values in import and export

In general, currency values crossing the boundaries of the platform are represented in the user’s session currency and formatted in the user’s locale.

Import

Currency values are imported as strings, just like other fields. The default transform mapping to a currency field uses `setDisplayValue()`. The expected format for this function is:

- A number formatted in the user’s locale. The number is taken as a value in the user’s session currency, for example, 1,234.56.
- The number prefixed by the three-letter currency code separated by a semicolon, for example, EUR 1.234,56.

This behavior can be customized in transform map scripts.

Export

Currency values are exported in the user’s session currency. They are formatted in the user’s locale, except when exporting as XML. When exporting currency in XML, the value is in the reference currency value with no formatting.

Default currency values in scripts

You can use currency fields in scripts.

These methods are available on GlideElement objects.

To display currency values, use the `getDisplayValue()` display API. To work with currency values in any way other than display, use the APIs that return/accept unformatted numbers.

**Note:** Before performing calculations on the value, do not use the `getDisplayValue()` methods and then process the string to remove formatting information.

Methods such as `getValue()` and `getCurrencyValue()` return unformatted numbers as strings. To obtain the floating point value, use the JavaScript function `parseFloat()`, and then use resulting value to perform calculations. To obtain the currency associated with these values, use the APIs that return the currency code. You can also use the `getCurrencyCode()` methods to determine a field’s currency.

```javascript
var rate = parseFloat(current.base_rate);
var currencyCode = current.base_rate.getCurrencyCode();

Use the `setValue()` method to set the value of a currency field. If this currency is the user’s session currency, use a plain number or the floating point number of a string containing it. Otherwise, prefix the value with the 3-letter ISO currency code.

```javascript
var totalCost = rate*current.hourly_rate;
current.total_cost.setValue(currencyCode + ";" + totalCost);
```  

You are working with the reference currency value when you use GlideAggregate on currency or price fields. Be sure to convert the aggregate values to the user's session currency for display. The resulting value may not be what you expect. The conversion rate used for the currency or price field value, and for its reference currency, which is used for the aggregation, may have changed.

When you delete a record containing a currency value, the platform deletes any associated currency records.
Note: Do not use `deleteMultiple()` on tables with currency fields. Always delete each record individually.

Currency values contain four decimal places.

- APIs that return values such as `getValue()` return up to four decimal places. Trailing zeros are always removed.
- APIs that return display values such as `getDisplayValue()` have at least two decimal places and up to four decimal places.
- GlideAggregate returns four decimal places.

You can have the system use two decimal places. When you set it to two decimal places, numeric values returned by the API contain two decimal places. Although currency conversion rates may have more decimal places, currency fields store only two decimal places. APIs that accept numeric values round decimal places to two places.

- APIs that return values such as `getValue()` return up to two decimal places. The trailing zeroes are removed for values read from the database, but if a value such as 00 is set later, 1.00 can be returned. The number of trailing zeros returned is not consistent.
- APIs that return display values such as `getDisplayValue()` contain up to two decimal places. It could sometimes return two places even for values such as 7.10, but could remove trailing zeros at other times. The number of trailing zeros returned is not consistent.
- GlideAggregate returns two decimal places.

Note: To learn how to change the number of decimal places used by the system, see Change default currency decimal places.

The following example, the user’s locale is set to German (de.DE), and the reference currency set to USD. The values use a currency value of 21345.67 in Japanese yen, 1563.72 in Euros, and 1152.48 in US dollars.

### Methods to access currency fields

<table>
<thead>
<tr>
<th>Method name</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>getValue()</code></td>
<td>Returns the currency value in the user's session currency as an unformatted number.</td>
<td>1563.72</td>
</tr>
<tr>
<td><code>getReferenceValue()</code></td>
<td>Returns the currency value in the reference currency as an unformatted number.</td>
<td>1152.48</td>
</tr>
<tr>
<td><code>getSessionValue()</code></td>
<td>Returns the currency value in the user's session currency as and unformatted number.</td>
<td>1563.72</td>
</tr>
<tr>
<td><code>getCurrencyValue()</code></td>
<td>Returns the currency value as entered as an unformatted number.</td>
<td>21345.67</td>
</tr>
<tr>
<td><code>getDisplayValue()</code></td>
<td>Returns the currency value in the user's session currency, formatted in the user's locale with a currency symbol.</td>
<td>€1.563,72</td>
</tr>
<tr>
<td><code>getSessionDisplayValue()</code></td>
<td>Returns the currency value in the user's session currency, formatted in the user's locale with a currency symbol.</td>
<td>€1.563,72</td>
</tr>
<tr>
<td><code>getReferenceDisplayValue()</code></td>
<td>Returns the currency value in the reference currency, formatted in the user's locale with a currency symbol.</td>
<td>$1,152.48</td>
</tr>
<tr>
<td>Method name</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td><code>getCurrencyDisplayValue()</code></td>
<td>Returns the currency value as entered formatted in the user's locale with a currency symbol.</td>
<td>¥21.345,67</td>
</tr>
<tr>
<td><code>getCurrencyString()</code></td>
<td>Returns the currency value as entered as an unformatted number, prefixed by the 3-letter ISO currency code, separated by a semicolon.</td>
<td>JPY 21345.67</td>
</tr>
<tr>
<td><code>getCurrencyCode()</code></td>
<td>Returns the 3-letter ISO currency code for the currency value as entered.</td>
<td>JPY</td>
</tr>
<tr>
<td><code>getSessionCurrencyCode()</code></td>
<td>Returns the 3-letter ISO currency code for the user's session currency.</td>
<td>EUR</td>
</tr>
<tr>
<td><code>getReferenceCurrencyCode()</code></td>
<td>Returns the 3-letter ISO currency code for the reference currency.</td>
<td>USD</td>
</tr>
<tr>
<td><code>setValue()</code></td>
<td>Sets the currency value as:</td>
<td>4369.21 or JPY 4369.21</td>
</tr>
<tr>
<td></td>
<td>• An unformatted number taken as a value in the user's session currency.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• An unformatted number prefixed by a 3-letter currency code separated by a semicolon.</td>
<td></td>
</tr>
<tr>
<td><code>setDisplayValue()</code></td>
<td>Sets the currency value as:</td>
<td>4369.21 or JPY 4369.21</td>
</tr>
<tr>
<td></td>
<td>• A number formatted in the user's locale that is taken as a value in the user's session currency.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• A number formatted in the user's locale prefixed by a 3-letter currency code separated by a semicolon.</td>
<td></td>
</tr>
</tbody>
</table>

**Default currency conversions**

Currency values can be converted to other currencies when stored and accessed. Conversions can happen in these situations.

- The currency value converts to the reference currency when stored, whether on insert or update. The reference currency value is saved as well as the currency value.
- The currency value converts to the user’s session currency for display.
- The value entered into a filter converts to the reference currency using the currency specified in the filter.

Conversion rates are stored in the fx_rate table. Each record contains the conversion rate from a given currency to the Euro. The rates are updated daily from the ECB website by a scheduled job called ECB Exchange Rate Load.

A currency conversion from one currency to another involves two rates.

- Actual: In the fx_rate table, each record contains the conversion rate from a given currency to the Euro.
- Expected: In the fx_rate table, each record contains the conversion rate from the Euro to the given currency.

Whenever you perform a conversion, it uses the latest conversion rates. Therefore, calculations can potentially yield unexpected results. For example:
• Different currency values can have different rates applied to them while storing the reference currency value. Therefore, aggregation can combine values at different rates and convert back at another rate.
• A filter value is converted at current rates while the values it filters in the database can be converted at different rates. A filter for $100 at today’s rate can match a value of $99 obtained at yesterday’s rates.

**Note:** For display purposes, the currency value used is what the user entered converted to session currency. However, for aggregation and filtering, the reference currency value is used. Using the reference currency enables currency values converted at different rates to be compared together.

### Schedule the rate update job

Schedule the Retrieve System Rates job to perform a nightly download of currency-conversion tables from the European Central Bank.

You can adjust the frequency of this behavior or disable it entirely. For information about turning off the regularly scheduled update and maintaining the Exchange Rate table manually, see Use your own currency-conversion rates.

1. Navigate to **System Scheduler > Scheduled Jobs**.
2. Open the job named **Retrieve System Rates**.
3. Modify the schedule, as needed.

   After the job runs, it stores and loads the rates from the Exchange Rate [fx_rate] table. Navigate to **System Localization > Exchange Rates** to see them.

### Use your own currency-conversion rates

All currency conversions are based on the rates stored in the Exchange Rate table. You can turn off the regularly scheduled update from the European Central Bank (ECB), and maintain the table manually.

ECB Exchange Rate Load loads exchange rates from the ECB for the following currencies:

[http://www.ecb.int/stats/eurofxref/eurofxref-daily.xml](http://www.ecb.int/stats/eurofxref/eurofxref-daily.xml)

If ECB does not supply the daily rates for a specific currency, you can manually enter rates into the Exchange Rate table. Use an import set, or another service (for example, JSON or SOAP) that offers upload of more currency rates. You can then add a similar scheduled job to update these currencies.

1. Navigate to **System Scheduler > Scheduled Jobs**.
2. Open the job named **ECB Exchange Rate Load**.
3. In the **Trigger type** field, select **-- None --**.
4. Enter new exchange rates either manually or with an Import Set.

### Setting up defaults required for standard currency use

Set up the defaults required for use of standard currency fields in your instance.

### Control default currency field configuration and use in an instance

You can control how currency fields are configured and used in your instance.

These properties are available for currency fields.

**Note:** To open the System Properties [sys_properties] table, enter `sys_properties.list` in the navigation filter.
### Properties for default currency fields

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>glide.sys.audit_currency_value</strong></td>
<td>When <em>true</em>, currency fields in audit records are the value entered by the user, in the format <strong>USD; 1234.56</strong>. When <em>false</em>, the value is the numeric value in the session currency.</td>
</tr>
<tr>
<td></td>
<td>• Type: Boolean</td>
</tr>
<tr>
<td></td>
<td>• Default value: <em>false</em></td>
</tr>
<tr>
<td></td>
<td>• Location: System Property [sys_properties] table</td>
</tr>
<tr>
<td></td>
<td>• Learn more: <a href="#">Configure default currency fields in audit records</a></td>
</tr>
<tr>
<td><strong>glide.currency_price.use_all_fraction_digits</strong></td>
<td>When <em>true</em>, currency fields have four decimal places. When <em>false</em>, two decimal places are used.</td>
</tr>
<tr>
<td></td>
<td>• Type: Boolean</td>
</tr>
<tr>
<td></td>
<td>• Default value: <em>false</em></td>
</tr>
<tr>
<td></td>
<td>• Location: System Property [sys_properties] table</td>
</tr>
<tr>
<td></td>
<td>• Learn more: <a href="#">Change default currency decimal places</a></td>
</tr>
<tr>
<td><strong>glide.currency_price_optimizer.enabled</strong></td>
<td>When <em>true</em>, the optimizer is used. When <em>false</em>, the optimizer is not used.</td>
</tr>
<tr>
<td></td>
<td>• Type: Boolean</td>
</tr>
<tr>
<td></td>
<td>• Default value: <em>true</em></td>
</tr>
<tr>
<td></td>
<td>• Location: System Property [sys_properties] table</td>
</tr>
<tr>
<td></td>
<td>• Learn more: <a href="#">Configure the currency optimizer</a></td>
</tr>
<tr>
<td><strong>glide.currency_price_optimizer.min_rows</strong></td>
<td>Minimum number of rows in parent table needed for the optimizer. When fewer than this number of rows are present, the optimizer is not used.</td>
</tr>
<tr>
<td></td>
<td>• Type: Number</td>
</tr>
<tr>
<td></td>
<td>• Default value: <em>4</em></td>
</tr>
<tr>
<td></td>
<td>• Location: System Property [sys_properties] table</td>
</tr>
<tr>
<td></td>
<td>• Learn more: <a href="#">Configure the currency optimizer</a></td>
</tr>
<tr>
<td><strong>glide.excel.convert_to_user_currency</strong></td>
<td>When <em>true</em>, currency fields in a table are output in the user's session currency.</td>
</tr>
<tr>
<td></td>
<td>• Type: Boolean</td>
</tr>
<tr>
<td></td>
<td>• Default value: <em>false</em></td>
</tr>
<tr>
<td></td>
<td>• Location: System Property [sys_properties] table</td>
</tr>
<tr>
<td></td>
<td>• Learn more: <a href="#">Exporting currency fields to Excel</a></td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>glide.excel.fixed_currency_usd</td>
<td>When true, currency fields in a table are converted to US dollars.</td>
</tr>
<tr>
<td></td>
<td>• Type: Boolean</td>
</tr>
<tr>
<td></td>
<td>• Default value: false</td>
</tr>
<tr>
<td></td>
<td>• Location: System Property [sys_properties] table</td>
</tr>
<tr>
<td></td>
<td>• Learn more: Exporting currency fields to Excel</td>
</tr>
<tr>
<td>glide.system.locale</td>
<td>Value is of the format Language.Country where the language is an ISO 639 language code and the country is an ISO 3166 language code. Internally, this value is used as specified by Java. The system locale setting should be in the Java supported locales list.</td>
</tr>
<tr>
<td></td>
<td>• Type: String</td>
</tr>
<tr>
<td></td>
<td>• Default value: empty</td>
</tr>
<tr>
<td></td>
<td>• Location: System Properties &gt; System Localization</td>
</tr>
<tr>
<td></td>
<td>• Learn more: Locale settings</td>
</tr>
</tbody>
</table>

### Change default currency decimal places

You can specify the number of decimal places stored and used in currency fields and calculations.

Role required: admin

1. Navigate to sys_properties.list.
2. Find glide.currency_price.use_all_fraction_digits, and set to the desired value.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>false</td>
<td>Uses two decimal places. This value is the default.</td>
</tr>
<tr>
<td>true</td>
<td>Uses four decimal places.</td>
</tr>
</tbody>
</table>

### Configure default currency fields in audit records

You can control what currency value is stored in audit records.

Role required: admin

1. Navigate to sys_properties.list.
2. Find glide.sys.audit_currency_value, and set to the desired value.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>false</td>
<td>Value entered in the audit record is the numeric value in the session currency. It does not include the currency code. This value is the default.</td>
</tr>
<tr>
<td>true</td>
<td>Value as entered by the user in the format USD. For example, 1234.56.</td>
</tr>
</tbody>
</table>
Configure the currency optimizer

You can configure the system to use an optimizer for currency/price fields to speed up list view (reading currency/price values).

Role required: admin

1. Navigate to `sys_properties.list`.
2. To turn on the currency optimizer, find `glide.currency_price_optimizer.enabled`, and set to the desired value.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>false</td>
<td>Optimizer is not used.</td>
</tr>
<tr>
<td>true</td>
<td>Optimizer is used. This value is the default.</td>
</tr>
</tbody>
</table>

3. To set the minimum number of rows needed by the currency optimizer, find `glide.currency_price_optimizer.min_rows`, and set to the desired value.
   The default value is 4.

Setting up and operating FX Currency fields

Use FX (Foreign Exchange) Currency fields as an alternative to the standard (default) currency fields found in most applications. They are highly configurable, support use of custom rate tables, report aggregations, and provide for improved visibility into conversion calculations.

**Note:** You don't have to install a plugin to use FX Currency functionality. It's activated by default.

Use considerations

Use the FX Currency field type in place of the standard currency fields when you must:

- Support values expressed in multiple currencies, for example, EUR 100, JPY 200, USD 30, as values in a field. FX Currency fields provide better support for multi-currency applications than do standard currency fields.
- Control how the FX Currency field is configured, including specifying its internal behavior and currency value formatting.

To learn more about currency configuration, see Configuring FX Currency field behavior.

- Create custom conversion rate tables.
  
  To learn more about custom table rates, see Add conversion rates using a custom rate table.
- Have more control over when the actual currency conversion occurs. FX Currency values convert on demand only, making the conversion results much more transparent.

To learn more about currency conversions, see Understanding how FX Currency field conversions work.

- Provide greater transparency into currency conversion calculations. You can view and configure the calculation components, including conversion dates, reference currency, and number of displayed decimals.
- Build query conditions using FX Currency field values. For available query conditions, see Operators available for filters and queries.
- Access FX Currency fields through richer scriptable APIs.
- Aggregate currency values as entered by users, or aggregate them in selected reference currencies, for reporting purposes.
Important: You can add FX Currency fields to base and custom applications, and they work independently of existing standard currency fields. However, you can't convert or change a standard currency field to an FX Currency type field. No functions are available to convert standard currency fields to FX Currency fields, then migrate the data from one to the other.

Understanding FX Currency values in forms

In forms, the FX Currency field behaves like a dot walkable field in script. It consists of an entry field, and an accompanying list for selection of a currency code.

Specifically, FX Currency fields that appear on forms contain the following:

- An empty field for entry of a numeric currency value, formatted according to your assigned user locale. For example, in the US, it is formatted with two decimal places, for entry of cents.
  
  If this is a new record, the field is empty. If it is an existing record, the previous currency amount that you entered appears.

- A selection list of active currencies from the Currency [fx_currency] table. The default currency code is based on your user locale. You can select another currency for use during the entry session.
  
  For example, in the US, the default currency value, based on the user locale, is USD. You can select another currency code to use in the current entry session.

- An edit icon

  (\). Users with an assigned currency_instance_admin role can click it to edit currency detail in the accompanying Currency Instance [fx_currency2_instance] record.
Updating the Currency Instance record

If you have an assigned role of currency_instance_admin, you can review and edit the details of a currency entry in an FX Currency field. You can't edit the reference currency and value because they are calculated automatically.

Role required: admin, currency_instance_admin, with ACL access to the FX Currency field.

1. Access the Currency Instance record using one of the following methods:

<table>
<thead>
<tr>
<th>Access method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct access from an FX Currency field</td>
<td>Click the edit icon that appears next to the FX Currency field in a transaction record.</td>
</tr>
</tbody>
</table>
| From the navigator bar            | a. Navigate to System Localization > FX Currency Configuration.  
                                      b. Click the Currency Instance record to edit. |

Note: Only users with an assigned admin role can access this selection from the navigator.
2. On the form, fill in the fields.

### Currency Instance

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Amount</strong></td>
<td>Currency amount that you entered into the FX Currency field, formatted according to the currency code in your user locale. The amount stores internally as a currency code and a numerical value of up to 12 digits in length. For example, USD; 1234.56.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>The currency value has two parts: the currency amount and a currency code. The amount stores as a decimal value, for example, 1234.56.</td>
</tr>
<tr>
<td><strong>Currency Code</strong></td>
<td>Three-letter ISO code that identifies the currency that you select for the currency amount. For example, USD for the US Dollar, or EUR for the Euro.</td>
</tr>
<tr>
<td><strong>Conversion Rate</strong></td>
<td>Conversion rate used to calculate the reference currency value. It converts a session currency value, expressed in one currency, to another, and stores as a reference to a record in the Currency Conversion Rate [fx_conversion_rate] table.  &lt;br&gt; &lt;br&gt; The conversion rate is based on the <strong>Conversion Rate Table</strong> and <strong>Conversion Date Source</strong> settings for the FX Currency field in the Rate tab of FX Currency Configuration. To learn more about these settings, see Configuring FX Currency field behavior. &lt;br&gt; &lt;br&gt; You change or select the conversion rate as needed.</td>
</tr>
<tr>
<td><strong>Reference Amount</strong></td>
<td>Calculated reference currency amount. The Now Platform converts the currency value entered into the <strong>Amount</strong> field into a common reference currency. It uses the settings in the <strong>Reference Currency Source</strong> and <strong>Reference Currency</strong> fields in <strong>System Localization &gt; FX Currency Configuration</strong> to do so. &lt;br&gt; &lt;br&gt; You can't change the calculated reference amount.</td>
</tr>
<tr>
<td><strong>Reference Currency Code</strong></td>
<td>Three-letter ISO code that identifies the reference currency, for example, USD, to which the entered currency value converted. You can't change the reference currency code.</td>
</tr>
</tbody>
</table>

3. Click **Save**.
Understanding how FX Currency field conversions work

You can use existing system currency rates or define a custom conversion rate table for use in FX Currency processing.

A currency conversion rate represents the conversion factor for exchanging one currency for another. The conversion rate is used when converting a currency value, expressed in one currency, to another currency. Conversions can occur for storage (for example, conversion to a reference currency) or for display (for example, conversion to a session currency).

When conversions occur

FX Currency fields expose the values inside the Currency Instance [fx_currency2_instance] record as dot walkable fields. You can access to all data held in an FX Currency field without any transformations. Conversions can happen in these situations:

1. Calculation of a reference value, calculated when you enter a currency value, whether on insert or update. The reference currency value is saved as well as the currency value as entered. Once this calculation takes place, the reference value is not recalculated.
2. Calculation of the session display value returned from `getDisplayValue()`, which performs conversions to the required currency.

The conversion rate is based on the settings of the Conversion Rate Table and Conversion Date Source fields in System Localization > FX Currency Configuration.

Note: To learn more about these settings, see Specify the rate table and date source for currency conversions.

Conversion rates

FX Currency conversion rates are stored in the following ways:

- System rate [fx_system_rate] table: Contains system conversion rates. Each record contains the conversion rate from the Euro to a given currency. The rates are downloaded daily from the ECB website by a scheduled job called Retrieve System Rates. To learn more, see Schedule the rate update job.
- Custom rate table: Contains custom currency conversion rates, and custom rate tables extend the Currency Conversion Rate [fx_conversion_rate] table. To learn more about creating custom rate tables, see Add conversion rates using a custom rate table.

Life cycle of records containing FX Currency fields

The behavior of FX Currency fields varies during the processing that occurs during the lifetime of a record containing them.

Insert / Update

The FX Currency field points to a Currency Instance [fx_currency2_instance] record. When you change the currency value in an FX Currency field, it determines the conversion rate and calculates the reference currency before:

- The before business rules run.
- The after business rules run, and it includes any further changes you may have made to the before business rules.
**Auditing**

Since an FX Currency field points to a Currency Instance record that stores multiple values, the audit string is a composite that contains this information. The string stored in the System Audit [sys_audit] table is in the format of `EUR;111.222;4555525f5553445f3230313931323033`, with the following values, separated by semicolons:

- Three letter ISO currency code. For example, `EUR`.
- Amount as an unformatted number. For example, `111.222`.
- System identifier (sys_id) for the conversion rate record in the Currency Conversion Rate [fx_conversion_rate] table. For example, `4555525f5553445f3230313931323033`.

When creating history lines for a user, the audited string is formatted, using the locale of the user. It's in the format of `€111.22;2019-12-03 17:00:00-3000-01-01 23:59:59;fx_system_rate`, with the following values, separated by semicolons:

- Formatted currency string in the user locale. For example, `€111.22`.
- Start span-End span, as expressed in the conversion rate record in the System Rate [fx_system_rate] table. For example, `2019-12-03 17:00:00-3000-01-01 23:59:59`.
- Name of the conversion rate table. For example, `fx_system_rate`.

**Dot-walkable Currency Instance fields**

You can dot-walk certain fields in the Currency Instance [fx_currency2_instance] record, and field values stored in the database are consistent with each other. However, in script, since fields can be changed individually, and you change only some of the fields, they can be inconsistent.

**Currency code**

The Currency field isn't a reference field, so you can set it to any value. However, if you enter an invalid currency code, an exception message is generated. An empty value is considered a session currency code.

**Query conditions**

You can add query conditions on dot-walked fields in the instance table. However, when the query condition value is in a special format with currency code and amount, it's treated as a compound condition on the dot walked fields. The value has to be in format `XYZ,abc` where:

- `XYZ` is a currency code, and
- `abc` is an amount.

For example, `USD, 12.34`.

A condition such as `cost>USD,12.34` is treated as `cost.currency>USD AND cost.amount12.34`.

When the second operand is another Currency2 field, the condition translates in a similar manner:

`cost1>cost2` is treated as `cost1.currency=cost2.currency AND cost1.amount>cost2.amount`. 
Understanding FX Currency values in lists and reports

By default, the currency values that appear in the FX Currency fields in lists and reports are the values that you directly enter into the FX Currency fields. For reports, the aggregations of FX Currency fields are, by default, reference currency values.

FX Currency values in list views

In lists, FX Currency values appear as a formatted currency string returned from `getDisplayValue()`.

- To learn more, see Identify the FX Currency field and its display parameters.

For an FX Currency field that depends on another FX Currency field, the currency value comes from the Currency Instance [fx_currency2_instance] record associated with the latter. The display value format is based on how you configured its display settings in System Localization > FX Currency Configuration.

Filtering FX Currency values in lists

In lists, FX Currency field filtering behaves differently than with standard currency fields. The filtering takes place using the currency type selected when a currency value is originally entered into an FX Currency field. It doesn't take reference currencies into account when you filter a list. So, if the unfiltered list contains FX Currency field entries in multiple currencies, a filtered list would only contain those records originally entered using the specified filtering currency.

- For example, if you entered a currency value in Euros (EUR) and the reference currency is US Dollars (USD), the reference currency value may appear in an unfiltered list.
- However, if you filter the list, and select USD as the currency, the currency value, originally entered in Euros, doesn't appear. In this case, only currency values originally entered in USD would appear.

Dependent FX Currency fields

Use of FX Currency view or dependent fields enable you to use alternate display configurations defined in System Localization > FX Currency Configuration for a particular FX Currency field. To learn more about FX Currency field configurations, see Configuring FX Currency field behavior.

When you create an FX Currency field, you can mark it as dependent on another FX Currency field. Marking an FX Currency field as dependent enables it to use the configuration settings for the original FX Currency field to display the amount values in different currency. Any changes that you make to the dependent field don't affect the original FX Currency field.

FX Currency reporting, aggregation, and group by

You can select FX Currency fields for inclusion on reports, and they display in the same manner as in list views.

- FX Currency fields appear as a formatted currency string returned from `getDisplayValue()`.
- If you set the Display Value Currency field in System Localization > All Properties to Display in Session Currency, the session currency assigned to the user running the report appears.

You can aggregate like reference currency values within a Currency Instance record. The following is the aggregated FX Currency data format in the Now Platform®:

© 2021 ServiceNow, Inc. All rights reserved.
Aggregate FX Currency value

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>Value of the aggregation. If the values being aggregated are FX Currency values, the returned value is in the format currency_code:currency_value, such as:</td>
</tr>
<tr>
<td></td>
<td>USD:134.980000</td>
</tr>
<tr>
<td></td>
<td>Otherwise, the returned value is just the currency value, such as: 134.980000.</td>
</tr>
</tbody>
</table>

**Note:** If the field contains FX Currency values of mixed currency types, the values cannot be aggregated. The value is returned as a semicolon (;).

For example, if the **Cost** field on a transaction record is an FX Currency field, you can group by **cost.amount** or **cost.currency**.

- Aggregation operations, such as **SUM**, translate as **SUM(amount)** or **SUM(reference_amount)**. The aggregation source determines the translation when the currency associated with the currency values in the grouping is the same.

  For example, the aggregate value returned by **GlideAggregate.getAggregate()** is a string of the format USD; 1234.56. The total currency value is expressed in the single reference currency that is associated with all currency values in the grouping.

- If there are different currencies associated with currency values in the grouping, then the aggregate value is empty. For example, if some of the currency values are in US Dollars, some are in Euros, and others in Yen, the aggregate value would be empty.

You can also use a Group By command on FX Currency fields.

- It is equivalent to grouping by currency and amount, or by reference_currency and reference_amount, as dictated by the aggregation source.
- The value of the grouping is available by dot-walking on the FX Currency field, or using an API such as **getDisplayValue()**.

**Setting up defaults required for FX Currency use**

Set up the defaults required for use of FX Currency fields in your instance.

Perform the following setup tasks to enable FX Currency processing:

**Add conversion rates using a custom rate table**

You can create a custom rate table to ensure repeatable and consistent calculations. In a custom rate table, you control the conversion rates and the frequency of rate conversions. If you don't define custom rate tables, FX Currency fields use the System Conversion Currency Rate [fx_system_rate] table, which updates rates daily from the ECB (European Central Bank) website.

Role required: admin, currency_admin

A conversion rate can be quoted in different ways.

- Direct conversion rate (A -> B) that may or not be invertible (that is, given rate R for A -> B, the rate for B -> A can be derived as 1/R).
• Indirect conversion rate through some intermediate currency (A -> C and C -> B).

1. Navigate to **System Definition > Tables**.
2. Click **New**.
3. In **Label** field, enter the name of the conversion rate.
   For example, Convert-US-Euro.
4. In the **Extends** field, select the Currency Conversion Rate [fx_conversion_rate] table.
5. Complete the remaining fields to create the new extended table.
   For more details, see **Create a table** for details.
6. Click **Submit**.
7. Navigate to the new table and fill in the fields on the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Currency</td>
<td>Currency to convert the rate conversion table from. For example, USD if you are converting from US Dollars.</td>
</tr>
<tr>
<td>To Currency</td>
<td>Currency to convert the rate conversion table to. For example, EUR if you are converting to Euros.</td>
</tr>
<tr>
<td>Span start</td>
<td>Date/time from which this currency rate is valid, for example, January 1, 2020 00:00:00.</td>
</tr>
<tr>
<td>Span end</td>
<td>Date/time to which this currency rate is valid, for example, January 30, 2020 23:59:59.</td>
</tr>
<tr>
<td>Order</td>
<td>Order in which a currency conversion selects currency rates when their time spans overlap. For a date/time and a currency pair, if there are multiple rates with a Span start less than or equal to the date/time, and Span end greater than or equal to the date/time, the currency conversion selects the lowest order rate.</td>
</tr>
<tr>
<td>Rate</td>
<td>Actual conversion rate, stored as a decimal with six decimal places.</td>
</tr>
</tbody>
</table>

8. Click **Update**.

After you create the custom rate table:

1. Manually populate the table, or import data to populate it.
2. To use this rate table on a global basis, change the glide.currency2.system_rate_table system property.
   To use it for a specific FX Currency field, change the Conversion Rate Table field setting in **System Localization > FX Currency Configuration**.

**Configuring FX Currency global settings**

Before setting up and using FX Currency, review the related system properties to confirm or modify its default behavior.

Role required: admin

The global defaults you establish in system properties apply the configuration option to all FX Currency fields. You can then customize them for specific dictionary attributes in **System Localization > FX Currency Configuration**. When you create a currency configuration, it applies those settings only to the FX Currency field that you add it to. To learn more about FX Currency configurations, see **Configuring FX Currency field behavior**.
FX Currency configuration settings for specific FX Currency fields take precedence over system properties. Administrators can set a global configuration for a property, and then apply exceptions on a field-by-field basis.

- If you change system defaults, except for `display_digits` and `display_value`, the changes apply to updated and new values only.
- Existing values and data don't change but rather display differently, depending on configuration.

**CAUTION:** Don't edit the Currency [fx_currency] table directly. The system maintains this table and your changes could have unintended consequences.

1. Navigate to **System Localization > All Properties.**
2. Review the system defaults and make any desired changes.

### FX Currency field properties and attributes

<table>
<thead>
<tr>
<th>System property</th>
<th>FX Currency configuration mapping</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.currency2.display_digits</td>
<td>currency_display_digits</td>
<td>Default number of digits displayed in FX Currency fields.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> In a form, FX Currency fields display the number of digits you enter, up to 12 digits in length.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Type:</strong> Number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Default value:</strong> -1, or currency default</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Available options:</strong> 0–12</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Develop:</strong> GlideCurrencyFormatter</td>
</tr>
<tr>
<td>glide.currency2.display_value</td>
<td>currency_display_value</td>
<td>Default currency display value returned from <code>getDisplayValue()</code>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Type:</strong> String</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Default value:</strong> as_entered</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Available options:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• as_entered: Currency value as entered by the user</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• in_session_currency: Currency value as entered by the user and converted to the session currency</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• in_reference_currency: Currency value as entered by the user converted to the reference currency</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Develop:</strong> GlideCurrencyFormatter</td>
</tr>
</tbody>
</table>
### System property

<table>
<thead>
<tr>
<th>glide.currency2.system_rate_table</th>
<th>conversion_rate_table</th>
<th>Conversion rate table used to perform currency conversions. By default, the source for currency conversions is the System Currency Conversion Rate [fx_system_rate] table, which stores the daily reference rates retrieved from the European Central Bank. If you have defined a custom rate table, you can change the rate table used in currency conversions.</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>Type</strong>: String</td>
<td></td>
<td>• <strong>Default value</strong>: fx_system_rate</td>
</tr>
<tr>
<td>• <strong>Available options</strong>:</td>
<td></td>
<td>• <strong>Learn more</strong>: Understanding how FX Currency field conversions work and Default currency conversions</td>
</tr>
<tr>
<td>• Any table that extends the</td>
<td></td>
<td>• <strong>Develop</strong>: GlideCurrencyConverter GlideCurrencyExchangeValue</td>
</tr>
<tr>
<td>Currency Conversion Rate table</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[fx_conversion_rate]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>glide.currency2.default_reference_currency</th>
<th>reference_currency</th>
<th>Three-digit ISO currency code used for the reference currency. The default reference currency for FX Currency fields is the system reference currency.</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>Type</strong>: String</td>
<td></td>
<td>• <strong>Default value</strong>: If you set glide.system.reference_currency to true, the three-digit ISO currency code determined by glide.system.reference_currency.code.</td>
</tr>
<tr>
<td>• If set to false, the system locale is the default.</td>
<td></td>
<td>• <strong>Learn more</strong>: Session and reference currency</td>
</tr>
<tr>
<td>• <strong>Develop</strong>: GlideElementCurrency2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Add an FX Currency field to a table

Before using and configuring an FX Currency field, you first add it an existing table, or to a new one, in **System Definition > Tables**.

Role required: admin
For example, you create a new custom table, named `transactions`, that stores transactional information and contains an FX Currency field called `cost`.

1. Follow the normal procedures to add a table, or access an existing table. To learn more about creating and modifying tables in an instance, see Create a table.

2. In the **Columns** section, use the **Table Columns** embedded list to add columns to the table.

3. In the **Column label** field, enter the column name. For example, `cost`.

4. In the **Type** field, select **FX Currency** as the field type.

5. As needed, enter other required parameters.

6. Click **Submit**.
Configuring FX Currency field behavior

After establishing global currency defaults, you can create custom FX Currency configurations for specific table fields. Identify the table fields that use FX Currency, and define how currency conversion calculations should be performed, displayed, filtered, and aggregated.

For each selected field that uses FX Currency, you configure settings that:

- Govern decimal precision and currency display in lists, forms, and reports.
- Identify the reference currency code for converting currency values entered into an FX Currency field into a common currency for report aggregations.
- Identify the rate table and data source to use for currency conversions.
- Specify the rate and target fields to use for filtering custom conversion rates.

**Note:** When you create a currency configuration, it applies those settings only to the FX Currency field that you add it to. An FX Currency configuration takes precedence over global system properties that you established in `System Localization > All Properties`.

To learn more about global currency defaults, see Configuring FX Currency global settings.

You can change the defaults at any time. Doing so doesn't affect existing values, but it can make working with existing values difficult.

- For example, if you modify the **Reference Currency** field in the Currency tab, existing instance records have the old reference currency, but new instance records have the new reference currency. You can't perform an operation such as sum aggregation because the reference values are in different currencies.
- However, because the actual reference currency in the Currency Instance [fx_currency2_instance] table is accessible in an FX Currency field, you can use any script that performs this aggregation.

Identify the FX Currency field and its display parameters

Specify the table, and the field within the table (for example, cost), that the FX Currency configuration applies to. Then, select the decimal precision and currency display parameters for the field.

Role required: admin, currency_admin

2. Click **New**.
3. In the **Table** field, select the table that contains the FX Currency dictionary attribute.
   - For example, if you created a custom table that stores transactional information and contains an FX Currency field, select it from the table listing. To learn more about creating tables in an instance, see `Create a table`.
4. In the **Field** field, select the column with the FX Currency field type.
   - For example, if you created a custom table column for entry of the transaction cost, select it from the listing of fields for the table.
5. Click **Save**.
6. Click the Display tab.
7. In the **Display Digits** field, select the number of digits that should appear after the decimal point in lists and reports.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Currency Default</strong></td>
<td>Number of digits that appear on lists and forms, based on what is appropriate and customary for the specified currency itself. For example:</td>
</tr>
<tr>
<td></td>
<td>• USD: Two digits appear after the decimal, for example, 12.33.</td>
</tr>
<tr>
<td></td>
<td>• Dinar: Three digits appear after the decimal, for example, 69.535.</td>
</tr>
<tr>
<td></td>
<td>• Yen: No digits appear after the decimal, because the Yen uses no cents and numbers round to the next latest value. For example, a calculated currency value of 69.535 rounds up to, and appears as, 67 Yen.</td>
</tr>
<tr>
<td></td>
<td>0–12 Specific number of digits that should appear after the decimal, with selectable values from 0 through 12. If you select more than 1, it pads the values with zeroes.</td>
</tr>
<tr>
<td></td>
<td>• For example, if you select 3, and the calculated value is 1.1, the currency value appears as 1.100.</td>
</tr>
<tr>
<td></td>
<td>• If you select 5, this value appears as 1.10000.</td>
</tr>
</tbody>
</table>

Note: In a form, FX Currency fields display the number of digits as entered by the user, up to 12 digits in length.

8. In the **Display Value Currency** field, select what currency value appears in the designated FX Currency field on forms and lists.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use Global Default</strong></td>
<td>Use the global default you established in the glide.currency2.display_value system property in System Localization &gt; All Properties.</td>
</tr>
<tr>
<td><strong>Display As Entered</strong></td>
<td>Currency value, as entered into the designated FX Currency field. For example, if the user locale is US Dollars, the value appears in Euros if they select the Euro as the currency during an entry session.</td>
</tr>
<tr>
<td><strong>Display in Session Currency</strong></td>
<td>Currency value entered into the designated FX Currency field, converted to the session currency.</td>
</tr>
<tr>
<td></td>
<td>• For example, if the user locale is the United States, the session currency appears in US Dollars.</td>
</tr>
<tr>
<td></td>
<td>• If the user locale is Japan, the session currency appears in the Yen.</td>
</tr>
<tr>
<td></td>
<td>To learn more about the user locale, see Locale settings.</td>
</tr>
<tr>
<td><strong>Display in Reference Currency</strong></td>
<td>Currency value entered into the designated FX Currency field, converted to the reference currency designated in the Reference Currency field in the Reference tab.</td>
</tr>
<tr>
<td></td>
<td>For example, if you enter the currency amount in Euros, it converts to and appears in US Dollars if that is the designated reference currency. To learn more the reference currency, see Set the reference currency.</td>
</tr>
</tbody>
</table>

9. In the **Aggregation Source** field, select the currency type to use when aggregating currency amounts for the designated field on reports.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use Global Default</strong></td>
<td>Use the global default you established in the glide.currency2.default_reference_currency property in System Localization &gt; All Properties.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>As Entered Values</td>
<td>Currency values, as entered into the designated FX Currency field. <strong>Note:</strong> If you select this option, you may experience situations where amounts entered in dissimilar currencies can’t be aggregated on reports. For example, if you enter currency amounts in US Dollars, Yen, and Euros, the amounts can’t be properly aggregated, or may result in erroneous totals.</td>
</tr>
<tr>
<td>Reference values</td>
<td>Currency values, as entered into the designated FX Currency field, converted to the reference currency you designate in the Reference Currency field in the Reference tab. For example, if you designate USD as the reference currency, values entered into this field convert to the reference currency, regardless of the currency you entered them in. The currency values that appear on reports are the aggregated converted reference values.</td>
</tr>
</tbody>
</table>

10. **Click Save.**

**Set the reference currency**
Set the reference currency for the designated FX Currency field. The Now Platform uses the reference currency to convert values entered into the FX Currency field into a common currency for report aggregation purposes.

Roles required: admin

1. Click the Currency tab.

2. In the **Reference Currency** field, select the three-digit ISO currency code used for the reference currency. For example, select **USD** if the currency values expressed in various currencies convert into US Dollars for report aggregation.

To use the global reference currency default you established in the `glide.currency2.default_reference_currency` property in **System Localization > All Properties**.

3. In the **Reference Currency Source** field, designate the source of the reference currency.
   - To use as the source of its reference currency when creating or updating a currency value for this FX Currency field, select the dot-walked field.
   - For example, `Cost` is an FX Currency field, and `my_currency` is a reference or string field in the Currency [fx_currency] table that contains a currency code such as USD.
   - When you create an FX Currency configuration for the `Cost` field, you select `my_currency` as its reference currency.
   - If you do not want to select the reference currency from another field, select **--None--**.

4. **Click Save.**

**Specify the rate table and date source for currency conversions**
Identify the rate table and data source to use for currency conversions for the designated FX Currency field.

1. Click the Rate Table tab.

2. In the **Conversion Rate Table** field, select the rate table used for conversions of currency values in the FX Currency field:
   - To use the default system rate table you defined in the `glide.currency2.system_rate_table` property in System Localization > All Properties., select **System Currency Conversion Rate**. This table stores daily reference rates retrieved from the European Central Bank.

   To learn more about the system rate table, see Default currency conversions.
   - If you have defined a custom rate table, you can select it to use in currency conversions for the FX Currency field. To learn more about how to define custom rate tables, see Add conversion rates using a custom rate table.
3. In the **Conversion Date Source** field, select the field to use as the source of the date and time for the currency conversion for the FX Currency field:

   - To use the date and time at which the user performs the currency conversion, select **--None--**.
   - To use as the source of the date and time for the currency conversion, select the dot-walked field.

   For example, to perform the currency conversion based on the currency rates in effect, select a transaction date field. So, if you entered the transaction on July 15, and you perform the currency conversion on July 31, it uses the currency conversion rates in effect on July 15.

4. Click **Save**.

**Select the rate and target table fields used for filtering**

Optionally specify the rate table and target table fields to use for filtering conversion rate information.

For example, you maintain interfaces to several ERP systems, have currency conversion rates that are unique to each ERP, but you maintain all rates in a single table.

   - To identify rates for a specific ERP system, there is a **System** field in the rate table that contain entries identifying each ERP system, for example, ABC, XYZ. In the target table with the FX Currency field, you have a similarly named field for identifying the conversion rates required for specific ERP systems.
   - When you perform currency conversions, and the rate and target table field entries match, it uses the rates that are unique to that specific ERP.

1. Click the Rate Filter tab.
2. In the **Rate Table Field** field, select the field in the rate table to match against the specified target table field for conversion rate filtering.
   
   Select **--None--** skip use of a rate table field for conversion rate filtering.
3. In the **Target Table Field** field, select the field in the target table to match against the specified rate table field for rate filtering.
   
   Select **--None--** skip use of a target table field for rate filtering.

4. Click **Save**.

**FX Currency values in import and export**

In general, currency values crossing the boundaries of the platform represent whatever is returned by `getDisplayValue`. Usually this currency value is the default as entered by a user into an FX Currency field for a transaction.

**FX Currency import**

If using the default `setDisplayValue()` import method, FX Currency works in manner similar to the standard currency field. It imports a value such as `USD;1,234.56` as `setDisplayValue("USD;1,234.56")`. It then parses the value as a three letter ISO currency code, followed by a semi-colon, followed by a number formatted in the locale of the user. This method should work for most use cases.

Defaults for other Currency Instance fields come from FX Currency field configuration you defined in **System Localization > FX Currency Configuration**. To explicitly set these fields, you can use a custom import script that sets those fields to desired values, possibly using values from another import column.

There are various ways to import FX Currency data.
### FX Currency export

There are various ways to export FX Currency data.

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show XML</td>
<td>Shows an XML file with instance records for each FX Currency field bundled inside the XML payload.</td>
</tr>
<tr>
<td>Export to XML</td>
<td>Shows an unload XML with unloads for all instance records.</td>
</tr>
<tr>
<td>Export to Excel/PDF</td>
<td>Uses the default method of exporting data that extracts data from fields using <code>getDisplayValue()</code>. For FX Currency fields, using this method returns a formatted currency string of the form $1,234.56. To access specific information inside an FX Currency field directly without any transformations, simply export that column using dot walking.</td>
</tr>
</tbody>
</table>

### System localization

Localization allows administrators to accommodate users from a variety of different countries, using different languages and currencies, within the same instance.

A digital guidebook for localization is available on the ServiceNow® Developer Site: ServiceNow Application Localization

### Define locales

The base system allows you to specify your locale so information such as dates, times, and currencies display properly based on your location.

**Note:** Functionality described here requires the Currency Support for Service Catalog Plugin plugin. This plugin is automatically installed for new instances.

By default, the base system uses US standard formatting where the current default is the US dollar sign ($) displayed with two decimal places: $100.00. By customizing your locale, you can make things such as currency appear as you expect. For example, in France, you may want to see 100,00 € instead of $100.00.

How you display and utilize various locale information within your application form depends on how you want to use the information. For example, if you make a country field a reference field, then users can select from predetermined options. Also, script logic can then use the predetermined values of those options. If you want to avoid bad values or want to run scripts based on these values, use a reference field. If the country field is a simple string field, then users can enter whatever information they desire. Most companies restrict such free-form input to administrators or implementers who are setting up features and core company data. For example, do you want the country name to be “United States of America”, “USA”, “United States”, or “US.”
Set the instance locale

Set the instance locale using a locale code.

Role required: admin

1. Navigate to System Properties > System Localization.
2. Enter the locale code to use under Locale code to use for localization. Format is [language code]. [country code] (e.g. en.GB for Britain, fr.FR for France, de.DE for Germany, or ja.JP for Japan).

<table>
<thead>
<tr>
<th>Country</th>
<th>Locale code</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>en.US</td>
</tr>
<tr>
<td>Great Britain</td>
<td>en.GB</td>
</tr>
<tr>
<td>France</td>
<td>fr.FR</td>
</tr>
<tr>
<td>Germany</td>
<td>de.DE</td>
</tr>
<tr>
<td>Japan</td>
<td>ja.JP</td>
</tr>
</tbody>
</table>

3. Click Save.

Language internationalization support

The ServiceNow platform supports multiple languages, using UTF-8 for international characters. Language support is available when at least one language plugin has been activated, as described in Activate a language.

When a user logs in, the language for the instance session is determined by the following logic:

1. If the language selection at login is enabled, that language is used.
2. If not, the language preference selected using the language picker in the header bar is used.
3. If not, the language setting in the User [sys_user] table is used.
4. If none of the above are true, the system default language is used.

Some areas of the system are not translated, including the following areas:

- Journal fields
- Report titles
- Any field that stores free-form text

These fields remain in the language used to create them.

Additionally, the following names are not translated:

- Product names
- Application names
- Plugin names
- Spoke names

The English version of these names is always kept, even when they are used in other contexts. For example, "Service Portal properties" might be translated into Dutch as "Service Portal eigenschappen." Feature names are translated, however.
When creating a custom field, you must add the labels in the Field Label table because they are not added automatically.

**FAQ**

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Will fields that I created or edited myself be translated?</td>
<td>The Now Platform does not perform translations. ServiceNow only provides translations of strings that the company itself has created. When you create a field, a message, or other textual UI content, translate this content manually.</td>
</tr>
<tr>
<td>I am not seeing journal fields translated.</td>
<td>Translation tables are not provided for user-defined string fields, such as short description, additional comments, and report titles. These fields can appear only in the language they were created in.</td>
</tr>
</tbody>
</table>

**Activate a language**

By default, the language supported by the platform is American English. You can activate the plugin for other supported languages if you have the admin role.

The following plugins are currently available:

- I18N: Brazilian Portuguese Translations
- I18N: Czech Translations
- I18N: Dutch Translations
- I18N: Finnish Translations
- I18N: French Canada Translations
- I18N: French Translations
- I18N: German Translations
- I18N: Hebrew Translations
- I18N: Hungarian Translations
- I18N: Italian Translations
- I18N: Japanese Translations
- I18N: Korean Translations
- I18N: Norwegian Translations
- I18N: Polish Translations
- I18N: Portuguese Translations
- I18N: Russian Translations
- I18N: Simplified Chinese Translations
- I18N: Spanish Translations
- I18N: Swedish Translations
- I18N: Thai Translations
- I18N: Traditional Chinese Translations
- I18N: Turkish Translations

In addition, the I18N: Internationalization plugin (com.glide.i18n) provides the elements necessary for translating an instance without any translation preloaded. This plugin is useful for translating an instance to a language other than those listed above. For more information on using the I18N: Internationalization plugin to translate an instance, see Translate to an unsupported language.

**Note:**

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Activating internationalization plugins for any of the available languages automatically activates the I18N: Knowledge Management Internationalization Plugin v2 plugin (com.glideapp.knowledge.i18n2).

- Product and Application Names are kept in English in localization plugins. Feature names are translated.

1. Navigate to System Applications > All Available Applications > All.
2. Find the plugin using the filter criteria and search bar.

You can search for the plugin by its name or ID. If you cannot find a plugin, you might have to request it from ServiceNow personnel. For more information, see Request a plugin.
3. Click Install, and then in the Activate Plugin dialog box, click Activate.

**Note:** When domain separation and delegated admin are enabled in an instance, the administrative user must be in the global domain. Otherwise, the following error appears: Application installation is unavailable because another operation is running: Plugin Activation for <plugin name>.

### Set default language for an instance

You can set the default language for an instance. Do this after activating the plugin for the desired language.

Before selecting a new default language, activate the plugin for the desired language in System Definition > Plugins. The default global language for the system is set in System Properties > System Localization. This property defines the language that users with a role see if a language is not specified in their user record. Users without a role see the default guest language, as described in User specific language.

---

#### Default language for the system (two character values):

<table>
<thead>
<tr>
<th>Language</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>en</td>
<td>English US</td>
</tr>
<tr>
<td>fr</td>
<td>Francais</td>
</tr>
<tr>
<td>es</td>
<td>Español</td>
</tr>
<tr>
<td>it</td>
<td>Italiano</td>
</tr>
<tr>
<td>de</td>
<td>Deutsch</td>
</tr>
<tr>
<td>en</td>
<td>English US</td>
</tr>
</tbody>
</table>

**Default language**

### User specific language

The user has several choices for identifying the language to be used for the instance, as described here.

To enable user-specific languages, first activate the I18N Translation plugins for the desired languages.

- **Language picker at login:** If user-specific language is enabled, users see a choice list on the login page to select their language. To control display of the choice list on the login page, navigate to System Properties > UI Properties and use the property Show the language select box on the login page to allow the user to specify the language they would like to be logged in with.
- **Language picker in the welcome banner (UI15):** When an internationalization plugin is enabled, users can select their language in the language picker in the welcome banner.
• **Language picker in the System Settings window (UI16):** Users can select their language in the General tab of the System settings window. Access this window by clicking the gear icon on the right edge of the banner.

• **Language setting on the user table:** If you have users that require a different language in addition to the global language, you can specify a language for them in User Administration > Users. If the Language field isn’t already on the form, you can configure the form and add it.

The **Language** field in the User [sys_user] table overrides the default global language for that user’s sessions.

![User language](image)

**Note:** Setting the language for the system guest user sets the language for both the login page and all users without a user role.

**Translation tables**

ServiceNow stores translation information in these tables.

- Languages [sys_language]
- Translated Name / Field [sys_translated]
- Message [sys_ui_message]
- Field label [sys_documentation]
- Choice [sys_choice]
- Translated Text [sys_translated_text]

To see which table contains a specific translated label, enable the display of translation prefixes. For more information, see Debug translations.
Note: The Languages table is available only after at least one I18N:Internationalization plugin has been activated.

Languages table

The Languages [sys_language] table contains a list of the languages for which translated text is available. To enable translation to a new language, add a record to the Languages table. The main fields for this table are:

- Name: language name.
- ID: two-character ISO 639.1 code for the language.
- Text Direction: direction of text in this language.
- Active: indicator that shows whether the language has been activated (true) for this instance or not (false).

Languages table

Configure a language as reading from right to left

Use the Text Direction field to configure a language that reads from right to left, such as Hebrew.

Role required: admin
Right-to-left language support is available only in the main user interface and on live feed. Other user interfaces and applications, such as the graphical Workflow Editor, reporting, CMS, chat, and the ServiceNow documentation sites, are not supported.

1. Navigate to **System Localization > Languages**.
2. Click **New**.
3. Enter the **Name** of the language, such as Hebrew.
4. Enter the two-character ISO 639.1 ID for the language. For example, Hebrew is `he`.
5. In the Text Direction field, select **Right-to-Left**.
6. Click **Submit**.

**Translated Name / Field table**

The Translated Name / Fields [sys_translated] table stores translated values for text fields where the field type is translated_field (see the dictionary entry).

This option is available for text fields up to 255 characters in length. Some examples are names, titles, and short descriptions. The main fields for this table are:

- **Table**: name of the table this translation applies to.
- **Element**: name of the field this translation applies to.
- **Label (translate)**: translated text that users see on forms and lists.
- **Language**: two-character ISO language code for this translated text.
- **Value**: English value that causes this translated text to be displayed.
The Messages [sys_ui_message] table contains the translations for informational messages, confirmation messages, error messages, and other types of system messages.

ServiceNow checks this table for translated text when a client script contains a getMessage call or a server script contains a gs.getMessage call. The main fields for this table are:

- **Key**: internal unique identifier of this message.
- **Language**: language the message is translated into.
- **Message**: translated text that users see.

The Messages table contains custom translatable text from the following sources when these texts are wrapped correctly:

- HTML in a UI page in a customer-created application
- Service Portal widget messages (including in surveys)
For more information about translatable custom content in the Messages table, see Custom translations.

**Message list**

<table>
<thead>
<tr>
<th>Key</th>
<th>Language</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>The following mandatory fields are not filled;</td>
<td>Dutch</td>
<td>De volgende verplichte velden zijn niet...</td>
</tr>
<tr>
<td>The following mandatory fields are not filled in: Apply Permissions To</td>
<td>Dutch</td>
<td>De volgende verplichte velden zijn niet...</td>
</tr>
<tr>
<td>The following mandatory fields are not filled in</td>
<td>Dutch</td>
<td>De volgende verplichte velden zijn niet...</td>
</tr>
<tr>
<td>Business values are not populated as there is no schedule applied</td>
<td>Dutch</td>
<td>De bedrijfswaarden zijn niet ingevuld om...</td>
</tr>
</tbody>
</table>

**Translated message**

**Field Label table**

The Field Label [sys_documentation] table stores the text of table names along with the singular and plural labels for each field in the table.

For each table name and field label, the Field Label table contains a record for each installed language. ServiceNow uses the table and field names from this table to display lists and forms in the proper language. The main fields for this table are:

- Table: name of the table this translation applies to.
- Element: name of the field this translation applies to.
- Language: two-character ISO language code for the translated text.
- Label: translated text that users see.
- Plural: plural of the label.
- Help: reserved for future use.
- Hint: text that pops up when the cursor rests on the field.
- URL: URL for a web page that provides information about the field. When a URL is provided, the field label displays a help icon ( ).
Translated field

Choices table


The main fields for this table are:

- Table: name of the table this translation applies to.
- Element: name of the field this translation is used for.
- Language: two-character ISO language code for the translated choice.
- Value: English description of this choice.
- Label: translated text that users see for this choice.
### Choice list

<table>
<thead>
<tr>
<th>Choice</th>
<th>Element</th>
<th>Value</th>
<th>Language</th>
<th>Priority</th>
<th>Label</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>sn_customerservice_case</td>
<td>priority</td>
<td>fr</td>
<td>1</td>
<td>1 - Critique</td>
</tr>
<tr>
<td></td>
<td>sn_vulc_result_group</td>
<td>priority</td>
<td>fr</td>
<td>1</td>
<td>mineur</td>
</tr>
<tr>
<td></td>
<td>sn_shn_notes</td>
<td>priority</td>
<td>nl</td>
<td>4</td>
<td>4 - Laag</td>
</tr>
<tr>
<td></td>
<td>change_request</td>
<td>priority</td>
<td>nl</td>
<td>2</td>
<td>2 - Hoog</td>
</tr>
<tr>
<td></td>
<td>rm_story</td>
<td>priority</td>
<td>fr</td>
<td>2</td>
<td>2 - Élevé</td>
</tr>
<tr>
<td></td>
<td>rm_story</td>
<td>priority</td>
<td>nl</td>
<td>1</td>
<td>1 - Kritiek</td>
</tr>
<tr>
<td></td>
<td>sn_vul_vulnerable_item</td>
<td>priority</td>
<td>fr</td>
<td>1</td>
<td>1 - Critique</td>
</tr>
</tbody>
</table>
The Translated Text [sys_translated_text] table stores translations for fields with the field type translated_text or translated_html (see the dictionary entry).

This field type is typically used for long text fields, up to 6500 characters in length, such as survey name and introduction. The main fields for this table are:

- Document: internal identifier of the record this translation applies to.
- Field name: field this translated text appears in, for example, Close notes.
- Language: language the text is translated into.
- Table Name: table this translation applies to.
- Value: translated text that the user sees.
### Debug translations

To debug translated strings in the UI, show translation prefixes before the strings. These prefixes indicate which strings can be translated and which table contains the string and translations. You can set translation prefixes to appear only in the current session or to appear in all sessions.

Role required: admin

- To enable translation prefixes on field labels for the current user session, navigate to **System Localization > Enable I18N Debugging**.
• To enable translation prefixes on field labels for all sessions, navigate to System Properties > System Localization and set Display translation prefix on translatable strings to Yes.

- Displays translation prefix on translatable strings.
  - Yes | No

• To disable translation prefixes that are enabled for the current session, either log out of the session or navigate to System Localization > Disable I18N Debugging.
• To disable translation prefixes that are enabled for all sessions, navigate to System Properties > System Localization and set Display translation prefix on translatable strings to No.

To apply the change, refresh your browser.

Translation prefixes and tables
Translation prefixes map to translation tables as follows.

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Table</th>
<th>Navigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRF</td>
<td>Translated Name / Fields [sys_translated]</td>
<td>System Localization &gt; Translated Names / Fields</td>
</tr>
<tr>
<td>MSG</td>
<td>Messages [sys_ui_message]</td>
<td>System Localization &gt; Messages</td>
</tr>
<tr>
<td>GMLD</td>
<td>Field Label [sys_documentation]</td>
<td>System Localization &gt; Field Labels</td>
</tr>
<tr>
<td>TRT</td>
<td>Translated Text [sys_translated_text]</td>
<td>System Localization &gt; Translated Text</td>
</tr>
<tr>
<td>CHC</td>
<td>Choice [sys_choice]</td>
<td>System Localization &gt; Choices</td>
</tr>
</tbody>
</table>

Note: A few strings may not display translatable prefixes. In this case, the string is not stored on any of these four tables. Examples of this behavior include:

- Text embedded in images, such as the buttons in the Service Catalog.
- Text defined by properties, such as the text which follows the banner.

Localize price fields
You can localize currencies for item prices and options.

Note: The system has the concept of a reference currency based on the global locale property. All currency values are automatically converted to the reference currency before aggregation or conversion. Do not change the global locale setting after you have data in the system. Changing the global locale setting after adding data to the system can cause aggregations to calculate and display incorrectly. See Currency administration for more information.

See Price fields for information on the types of price fields supported.
See Default currency values in scripts for information on using currency fields in scripts.
Localization settings

Localization settings control translation, currency, and locale settings in the instance.

The platform supports internationalization of language and localization of currencies and prices wherever they appear.

A digital guidebook for localization is available on the ServiceNow® Developer Site: ServiceNow Application Localization

Set up locations

If your organization supports more than one distinct location, you can configure these locations in the platform to help further identify users, assets, and incidents.

1. In the application navigator, navigate to **User Administration > Locations**.
2. Click **New**.
3. Complete the form with the necessary information then click **Submit**.
   
The new location is available as a reference anywhere you can specify one.

System localization properties

System properties to localize the instance for users from multiple countries.

Role required: admin

Some localization properties only appear after the I18N: Internationalization plugin is activated.

Navigate to **System Properties > System Localization**.

### Properties for system localization

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Show the language select box on the login page to allow the user to specify the language they would like to be logged in with.</strong></td>
<td>Enables language selection upon login.</td>
</tr>
<tr>
<td>glide.ui.login.language.select</td>
<td><strong>Options</strong>: Yes</td>
</tr>
<tr>
<td></td>
<td><strong>Default value</strong>: Yes</td>
</tr>
<tr>
<td></td>
<td><strong>Dependency</strong>: The I18N: Internationalization plugin must be active</td>
</tr>
<tr>
<td><strong>Text Search stemming language.</strong></td>
<td>Selects the language to match derived words in text search.</td>
</tr>
<tr>
<td>glide.ts.stemming_language</td>
<td><strong>Options</strong>: English, German, and French</td>
</tr>
<tr>
<td></td>
<td><strong>Default value</strong>: English</td>
</tr>
<tr>
<td></td>
<td><strong>Dependency</strong>: The I18N: Internationalization plugin must be active</td>
</tr>
<tr>
<td></td>
<td><strong>Learn more</strong>: Zing matches derived words with stemming</td>
</tr>
<tr>
<td><strong>Displays translation prefix on translatable strings.</strong></td>
<td>Adds a translation prefix on translatable fields to indicate where to find the string for translation.</td>
</tr>
<tr>
<td>glide.ui.i18n_test</td>
<td><strong>Options</strong>: Yes</td>
</tr>
<tr>
<td></td>
<td><strong>Default value</strong>: No</td>
</tr>
<tr>
<td></td>
<td><strong>Learn more</strong>: Debug translations</td>
</tr>
</tbody>
</table>
| Use a single currency model. Display all currencies in the same currency code, regardless of a user's locale, country, or language code. | Enable single currency mode.  
  **glide.i18n.single_currency**  
  **Options:** Yes | No  
  **Default value:** No  
  **Learn more:** Currency administration |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Default language for the system (two character values)</td>
<td></td>
</tr>
</tbody>
</table>
  **glide.sys.language**  
  **Options:** en, fr, es, it, de  
  **Default value:** en |
| If using the single currency model, display all currencies using this currency code. Currency codes use the ISO 4217 three letter format. |  
  **glide.i18n.single_currency.code**  
  **Options:** ISO 4217 three-letter currency code  
  **Default value:** USD  
  **Learn more:** Currency administration |
| Locale code to use for localization. | Determines the system's default currency into which all prices are automatically converted before other sums or conversions are performed. Changing this property after any price or currency fields have been given a value may result in improper conversion or prices that sum incorrectly.  
  **glide.system.locale**  
  **Options:** [language code].[country code] (for example, en.GB for Britain, fr.FR for France, de.DE for Germany, or ja.JP for Japan)  
  **Default value:** None  
  **Learn more:** Locale settings  
  **Note:** Do not change this value once a system has gone into production. If a user's locale must be changed, update the "Country code" field on the user record. |
| Add the labels, messages, or choices to the appropriate table in English with an ending of the language code for newly added customizations that are missing translations. (Translate and Learn). | Adds the current language suffix to UI elements such as labels and messages. Enabling the language suffix assists with translating new customizations.  
  **glide.translate.learn**  
  **Options:** Yes | No  
  **Default value:** No  
  **Dependency:** The I18N: Internationalization plugin must be active  
  **Learn more:** Use the translate and learn property |
| Spell checker dictionary to use for English users. | Sets the spell checker dictionary used in the system for English users.  
  **glide.spell.dictionary.en**  
  **Options:** Brazilian Portuguese, Dutch, English US, English UK, French, German, Italian, Portuguese, Russian, Spanish, and Thai  
  **Default value:** English US  
  **Learn more:** Locale settings |
Custom translations

You provide your own translations of applications you create and of modifications you make to the Now Platform®. You can also provide any translations to languages that ServiceNow does not provide translations for. The translation process varies depending on the type of item that you are translating.

The Now Platform does not provide any automatic translation capability. Instead, ServiceNow provides translations of the default platform in supported languages, as described in Activate a language. If you customize an instance and you want translations of the custom content, you have to provide those translations yourself.

The method of translation depends on the material that you are translating. Repeat the translation method whenever you edit or update content.

Translation methods and use cases

<table>
<thead>
<tr>
<th>What needs translation</th>
<th>Approach to take</th>
<th>Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field labels in a table for a customer-created application</td>
<td>First create English versions for all fields in the table. Then open the Field Labels translation table. Locate the records for the table in the application. Export the records, translate the appropriate fields, set the language field, and reimport through an import set.</td>
<td>Export and edit translation records. Alternatively, follow the procedure for translating individual labels in Translate a field label.</td>
</tr>
</tbody>
</table>
| HTML in a UI page in a customer-created application | 1. Create the English version. When creating the HTML in the UI Page form, wrap any translatable text in gs.getMessage calls.  
2. Create a Message [sys_ui_message] record for each English message with a corresponding key/value pair.  
3. Create additional Message records for each message for each other language. | Translate a client script message |
| Service Catalog items | 1. Navigate to System Properties > System Localization and set Display translation prefix on translatable strings to Yes.  
2. Create the item in English.  
3. Change the preferred language to a different language.  
4. Translate all the translatable items, now identified by translation prefix.  
5. Save the record. | To activate translation prefixes, see Debug translations. For translatable text fields, which are common in Service Catalog items, see Translating text fields. |
<table>
<thead>
<tr>
<th>What needs translation</th>
<th>Approach to take</th>
<th>Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Portal widget</td>
<td>1. Create the English version. Externalize any translatable text by surrounding the text with <code>$()$</code> wrappers.</td>
<td>• Translate a client script message</td>
</tr>
<tr>
<td></td>
<td>2. Create a Message [sys_ui_message] record for each English translatable text with a corresponding key/value pair.</td>
<td>• Internationalize a widget in Service Portal documentation</td>
</tr>
<tr>
<td></td>
<td>3. Create additional Message records for each piece of translatable text for each other language.</td>
<td>• For unofficial advice, see Building multi-lingual service portals</td>
</tr>
<tr>
<td>Edit a translation provided in a plugin</td>
<td>Export the records from the translation table. Edit them outside the translation table and reimport them. Do not edit the records directly, because your changes could be overwritten when you upgrade or zBoot your instance.</td>
<td>Export and edit translation records</td>
</tr>
<tr>
<td>Translate an instance to an unsupported language</td>
<td>Create a Choice [sys_choice] record for that language. Add other translation records through the Export and import set approach.</td>
<td>Translate to an unsupported language</td>
</tr>
<tr>
<td>Support Chat texts</td>
<td>Support Chat is mostly translated through the I18N language plugins. If you customize any Support Chat texts, follow the procedure for Service Portal widgets.</td>
<td></td>
</tr>
<tr>
<td>Emails and Surveys</td>
<td>System Localization does not cover email notifications or surveys. The usual approach is to create a separate version of each survey or notification in each language and use business rules to send the right language version to the right end user.</td>
<td></td>
</tr>
</tbody>
</table>

### Locate translatable strings

You have to provide your own translation of customer-created and customer-edited strings, such as field names and messages. In this case, locate the individual untranslated strings, translate them, and insert those translations into the correct tables.

The Internationalization language plugins contain translations of the UI string content that ServiceNow provides by default in your instance. The Now Platform does not perform translations. Whenever you have customized UI strings that you want to translate, you have to identify and translate these strings manually. To perform these translations, you must first take the following actions:

- Identify the strings that need to be translated.
- Identify which translation tables contain the strings.

#### Note:
Knowledge article translation uses a separate system which relies on the I18N:Knowledge Management Internationalization Plugin. If this plugin is not activated, Knowledge article translation falls back on the system described here, with translations kept in the Translated Text [sys_translated_text] table.
For more information about Knowledge Management internationalization, see Translation Management in the Knowledge Management documentation.

If you have a small amount of material to translate and you know where in the UI it is all displayed, consider using the debug functionality. This functionality consists of prefixes which you enable before all translatable strings. These prefixes show which translation table the strings are located in. For more information, see Debug translations.

For instances that contain a significant amount of customer-created UI, consider using one of the approaches described in the following topics:

**List non-translated items**

One method for easily translating customizations is to export the translated names and fields, messages, field labels, and choices that have records only for the English language. Export to any supported environment, translate the texts using your preferred translation environment, and reimport using import sets.

Role required: admin

Modules can be activated that correspond to the following translation tables, but list only records for which only an English version is available:

- Translated Name / Fields
- Messages
- Field Labels
- Choices

These modules are inactive by default. Activate them from the Activation Menu to make them available for export.

**Note:** This method does not identify strings that have been translated into at least one non-English language but are missing translations in other languages.

1. Navigate to System Definition > Application Menus.
2. Use the list editor to set the Active field to True for the modules whose order comes after Non-translated Items.
<table>
<thead>
<tr>
<th>Title</th>
<th>Table</th>
<th>Active</th>
<th>Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>Languages</td>
<td>Languages [sys_language]</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>Translated Name / Fields</td>
<td>Translated Name / Field [sys_translated]</td>
<td>true</td>
<td>100</td>
</tr>
<tr>
<td>Messages</td>
<td>Message [sys_ui_message]</td>
<td>true</td>
<td>200</td>
</tr>
<tr>
<td>Field Labels</td>
<td>Field Label [sys_documentation]</td>
<td>true</td>
<td>300</td>
</tr>
<tr>
<td>Choices</td>
<td>Choice [sys_choice]</td>
<td>true</td>
<td>400</td>
</tr>
<tr>
<td>Translated Text</td>
<td>Translated Text [sys_translated_text]</td>
<td>true</td>
<td>450</td>
</tr>
<tr>
<td>Non-translated Items</td>
<td></td>
<td>true</td>
<td>500</td>
</tr>
<tr>
<td>Translated Name / Fields</td>
<td>Translated Name / Field [sys_translated]</td>
<td>true</td>
<td>600</td>
</tr>
<tr>
<td>Messages</td>
<td>Message [sys_ui_message]</td>
<td>false</td>
<td>700</td>
</tr>
<tr>
<td>Field Labels</td>
<td>Field Label [sys_documentation]</td>
<td>false</td>
<td>800</td>
</tr>
<tr>
<td>Choice</td>
<td>Choice [sys_choice]</td>
<td>false</td>
<td>900</td>
</tr>
</tbody>
</table>
Note: Instead of Non-translated Items, your list might show a record titled Customizations. Activate that record and Save. After saving, the title shows Non-translated Items.

After the application navigator refreshes, the modules appear in the filter navigator beneath Non-translated Items.
3. View each of the lists and export it to any supported format, such as Microsoft Excel. For example, open **Non-translated Items > Translated Name/Fields**, select any column, and export the list. Translate the fields in the external application and reload the translations as an update set.

**Use the translate and learn property**

When the **glide.translate.learn** system property is set to true, the instance creates stub records in the translation tables when it encounters strings that have only an English version.

Activate the I18N: Internationalization plugin (com.glide.i18n) and at least one language. For more information, see [Activate a language](#).

Role required: admin

The instance creates stub translation records for strings only in forms and records that ServiceNow provides or that have been opened at least once. In practice, you need to know which modules contain untranslated customer-created strings to use this approach with customer-created content.

**Note:** Using this method prevents the use of the Export Untranslated Strings method. This method creates stub translation records and the method of exporting untranslated strings identifies only missing translation records.

1. Navigate to **System Properties > System Localization**.
2. Activate **Display translation prefix on translatable strings**.

   Displays translation prefix on translatable strings.

   [Yes | No]
3. Scroll down and activate the Translate and Learn property, as follows:
   
   Add the labels, messages, or choices to the appropriate table in English with an ending of the language code for newly added customizations that are missing translations. (Translate and Learn)  
   
   Yes | No

4. Click Save

5. Change your user language to one of the non-English languages installed on your instance.

6. Open each of the customer-created or customer-modified UI forms.
   
   The instance creates stub translation records for each untranslated but translatable string. These records are marked with the target language in the Label (translate) field, such as [fr].

7. Open each translation table and find the stub translation records.

**Untranslated customer-created HR modules**

For example: A user switches to the French language and opens a record. When loading the form, the instance looks at the Translated Field table to find the French translation for each field. If an appropriate translation record is not found, the instance automatically generates a stub record for that missing data, which can be manually translated.

The following HR application is missing translations for two modules:

![Image of HR application missing translations]

The suffix [fr] indicates that there is a French translation missing.
Note: These modules have been opened at least once already. Otherwise, the [fr] suffix would not appear.

Because translation prefixes are enabled, the prefix \textit{TRF:} indicates that the entry can be found in the Translated Name / Fields table. The following image shows untranslated modules, located using the filter [Label (translate)] [contains] [fr]:

![Untranslated modules](image)

\textbf{Example untranslated modules}

\textbf{Translate individual field labels and values}

When translating just a few field labels or values, such as when you add customizations to a translated instance, use the procedure that applies to the type of text being translated.

Three types of ServiceNow fields store translated strings:
• **Translated_field**: Stores field labels, related list names, and certain field values. The value of the translated_field replaces the label, list name, or field value when the user selects the matching language. Translated_field values have a one-to-many relationship with their associated keys. As a result, multiple records can reference one translated_field value.

• **Translated_text**: Stores long text values in plain text. The value of the translated_text replaces the plain text when the user selects the matching language. Translated_text values have a one-to-one relationship with their associated keys. As a result, only one record can reference a translated_text value.

• **Translated_html**: Stores long text values in HTML. The value of the translated_html replaces the HTML when the user selects the matching language. Translated_html values have a one-to-one relationship with their associated keys. As a result, only one record can reference a translated_html value.

All three translated field types support list sorting. To determine the field type, right-click the field on the form, select **Configure Dictionary**, and check the **Type** field.

ServiceNow stores the translated values as separate records and displays the proper value according to the end user’s language. You can translate an entire instance by exporting the translation tables and then importing the translated strings as described under **Export and edit translation records**.

**Note:** In addition to translated field types, currency fields display the same price in different currencies based on the user's language.

### Create a new choice record

This record allows users to select the language as a valid option in a User record and the language picker.

You must create a choice record for a new translation in the Choices [sys_choice] table.

1. Navigate to **System Localization > Choices**.
2. Click **New**.
3. Enter the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>What to enter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>sys_user</td>
</tr>
<tr>
<td>Element</td>
<td>preferred_language</td>
</tr>
<tr>
<td>Language</td>
<td>Enter the two-character ISO 639.1 code for the language that the user is currently using before they select the new language. The default is en.</td>
</tr>
<tr>
<td>Label</td>
<td>Enter the name of the new language selection as you want it to appear in the language picker. For example, Mongolian.</td>
</tr>
<tr>
<td>Value</td>
<td>Enter the two-character ISO 639.1 code for the new language that the user is selecting. For example, mn.</td>
</tr>
<tr>
<td>Sequence</td>
<td>Enter a number to determine what order the option appears in the choice list if you do not want to list choices alphabetically. For example, 5.</td>
</tr>
</tbody>
</table>

The following record allows a user who is using the Dutch localization of their instance to change languages to Mongolian:

- **Table**: User [sys_user]
- **Element**: preferred_language
• **Language**: nl
• **Label**: Mongoolse
• **Value**: mn

4. Click **Submit**.

**Create a new language record**

You must create a language record for your new translation in the Languages [sys_language] table.

Role required: admin

1. Navigate to **System Localization > Languages**.
2. Click **New**.
3. Enter the following fields.
   - **Name**: Enter the name of the language. For example, Turkish.
   - **ID**: Enter the two-character ISO 639.1 code for the language. For example, tr.
   - **Text Direction**: Select the direction that the instance should display the language in. For example Left-to-Right.

4. Click **Submit**.

**Translate a client script message**

Client scripts include a multi-line **Messages** field.

Use this field to enter message strings that the client script can use as a key to look up a localized message alternative from the Message [sys_ui_message] table. Add each message key on a separate line. The instance looks for a localized message string anytime the client script makes a getMessage(msg) call where the msg string matches a key in the **Messages** field.

For example, if you add the string **Please populate the Reason field** to the **Messages** field, then the instance will look for a localized string from the Message [sys_ui_message] table any time the client script calls:

```getMessage("Please populate the Reason field")```

Add a new record to the Message [sys_ui_message] table for each localized string.

1. Navigate to **System Localization > Messages**.
2. Click **New**.
3. Enter the **Message** fields for the localized message.
4. Click **Submit**.

**Translate a field label**

Field labels are the names that appear on forms and lists to describe the type of information the field contains.

The following procedure works best for translating individual field labels, such as those added with a customization. To translate large numbers of field labels, use the procedure described in **Translate the Interface**.

1. Navigate to the field on the form.
2. Right-click the field label and select **Configure Label**.
3. In the **Field Label** form, replace the English text with the text of the target language in the **Label**, **Plural**, and **Hint** fields.
4. Enter the two-character **Language** code of the target language.
5. Right-click the header bar and select **Insert**.
Clicking **Insert** creates a new record in the Field Label table for this field label in the selected language.

**Translate a field value**

Field values are the text entries that are used for fields with the type `translated_field`, such as the **Title** or **Hint** field in the `Module [sys_app_module]` table.

The following procedure works best for translating values for individual fields, such as those added with a customization. To translate large numbers of field values, use the procedure described in [Export and edit translation records](#).

1. Use the language picker in the header bar to switch to the desired language.
2. Navigate to the field on the form.
3. Enter the text of the target language for this value.

![Translated from “My Approvals”](image)
4. Click **Submit**.

   This creates a new record in the Translated Name / Field table for the selected language or updates the existing record.

**Translating text fields**

You can translate long pieces of text into the language of the user.

Translated text fields allow the same field to display different content based on the language of the user.

There are two different translated text fields:

- Translated Text
- Translated HTML

These fields operate the same as text and HTML fields respectively, except that they can store multiple inputs in multiple languages.

The most frequent use of translated text fields is in the Service Catalog (e.g. names, descriptions, or variables). If the Knowledge Management Internationalization Plugin is disabled, translated text fields are also used for Knowledge Base articles. For more information about Knowledge Management internationalization, see Translation Management in the Knowledge Management documentation.

**Translate long text content**

You can translate the content of translated text fields directly in the form where the content is specified.

Use the following procedure to translate the content for untranslated customer-created text fields. To edit existing text translations, export the records from the Translated Text table and follow the procedure in Export and edit translation records.

1. Open the record with the field that you want to translate.
2. Verify that the field whose content you want to translate is a translated_text or translated_html field.
   The following steps are one possible way to verify a field type:
   a) Right-click the label of the field and select Configure dictionary.
      In this example, the context menu has been opened for the Name field for a record in the Record Producer [sc_cat_item_producer] table.

Context menu for field

b) In the Dictionary Entry record that opens, confirm that the Type field is Translated Text or Translated HTML.
   In this example, you see that the Name field is of the type Translated Text.

Dictionary entry for field

c) Click back to the form.

3. Use the language picker to switch to the desired language.
4. In the relevant field, replace the English text with the text of the target language.
5. Click Submit.
The platform creates a new record in the Translated Text table for the active language. When a user selects this language, the field displays the translated content for this language. When a user selects English or a language without an associated Translated Text record, the field displays English content.

**Administering translated text fields**

There is a slight performance penalty associated with changing a normal HTML or text field into a translated HTML or text field. It is best only to use translated fields if the translated capability is required.

English language text is stored in the main table, but the values of other are stored in the Translated Text [sys_translated_text] table. Each translated field on every row has one or more entries in the sys_translated_text, one per language for which ServiceNow provides a translation.

For more information about the Translated Text table, see Translated text table.

**Translate a related list name**

Related lists appear at the bottom of forms. You can translate a related list name by configuring the list control.

Role required: personalize_control

1. Use the language picker to switch to the desired language.
2. Navigate to the related list on the form.
3. Open the list control for the related list by performing the appropriate action for the list version.

<table>
<thead>
<tr>
<th>Version</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>List v2</td>
<td>Right-click any column heading and select Configure &gt; List Control.</td>
</tr>
<tr>
<td>List v3</td>
<td>Open the list title menu and select List Control.</td>
</tr>
</tbody>
</table>

4. On the List Control form, replace the existing Label with the text of the target language.
5. Click Submit or Update.

The system creates a new entry in the Translated Name / Field [sys_translated] table or updates the existing entry for this language.

**Export and edit translation records**

Export the translations in a supported format. Work on the translations in your preferred translation environment, and import the new or edited translation records through import sets.

Role required: admin

In the following cases, translate strings in the UI outside of the Now Platform and import them through import sets:

- You have a significant amount of customer-created UI components and you want to translate these components into other languages.
- You want to modify translations that ServiceNow provides in internationalization plugins.
- You want to translate an instance into a language that ServiceNow does not support with internationalization plugins.

All translatable UI strings items are stored in translation table records. For more information, see Translation tables.

The only time you would translate UI directly in translation records is when you have a small amount of customer-created UI components and you know exactly where they are.

**Warning:** If you directly edit translation records that ServiceNow provides in internationalization plugins, your changes are lost when the instance is upgraded.

If you are translating customer-created components or you are modifying translations that ServiceNow provides in internationalization plugins, use the following steps.
**Note:** If you are translating an instance to a language that ServiceNow does not support with internationalization plugins, follow the procedure in Translate to an unsupported language.

1. If you are translating customer-created UI components, locate the translatable strings. Use the tools described in Locate translatable strings.
2. Export the relevant translation table records into a format (such as Excel) that can be easily manipulated. For more information about exporting a list of records, see List Export.
3. Within the exported document, translate the following fields in each row, depending on the translation table:

<table>
<thead>
<tr>
<th>Translation table</th>
<th>Fields to translate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field Labels</td>
<td>Label, Plural, Hint</td>
</tr>
<tr>
<td>Translated Name/Field</td>
<td>Label (translate)</td>
</tr>
<tr>
<td>Message</td>
<td>Message</td>
</tr>
<tr>
<td>Choices</td>
<td>Label</td>
</tr>
<tr>
<td>Translated Text</td>
<td>Value</td>
</tr>
</tbody>
</table>

4. Within each row, change the "Language" column to the two-character ISO code of the new language. In Translated Text records, type the full name of the language instead of the ISO code.
5. Save your changes.
6. Import the translated document back into the instance as an import set.

**Import a translation from an Excel spreadsheet**

The System Import Sets application contains four import tables and corresponding transform maps to assist with importing translations from an Excel spreadsheet.

1. Navigate to System Import Sets > Load Data.
2. Select Use Existing and the Table name that matches the type of data being imported, as follows.
   - For choices, select the [u_sys_choice] table.
   - For field labels, select the [u_sys_documentation] table.
   - For translated names and fields, select the [u_sys_translated] table.
   - For messages, select the [u_sys_ui_message] table.
   - For translated text, select the [u_sys_translated_text] table.
3. Select Upload an Excel file, and then click Browse to select the source Excel spreadsheet.
4. If appropriate, specify the Work sheet and Header row number.
5. Click Go.

The translations are now available in the appropriate Import Set Table.
6. Navigate to System Import Sets > Table Name and review the imported information to verify that the import was successful.
7. To transform the imported data into the corresponding table, navigate to System Import Sets > Run Transform.
8. Select the appropriate transform map, as follows.

**Note:** Make sure you choose a transform map that has the Run Business Rule option selected. If the transform map does not have this option selected, any customized translations you have may be overwritten during the next upgrade.

- For choices, select the Sys Choice Translation Map.
• For field labels, select the **Sys Documentation Translation Map**.
• For translated names and fields, select the **Sys Translated Translation Map**.
• For messages, select the **Sys UI Message Translation Map**.
• For translated text, select the **Sys Translated Text Translation Map**.

9. Click **Transform**.

**Translate to an unsupported language**

You can translate the interface of an instance to a language for which ServiceNow does not provide an internationalization plugin. Request ServiceNow to provide a file containing strings from the interface in the English language. Translate this file into your preferred language and import it to the instance.

Role required: admin

All interface items are stored as translatable strings in the translation tables. For more information, see **Translation tables**.

By default, these translation tables only contain English strings. To populate these tables with translated strings:

1. Create a Choice [sys_choices] record so users on that language can choose the new language.
   a) Navigate to **System Localization > Choices** and click **New**.
   b) Fill in the following fields:

   **Choice record fields to select the new language**

<table>
<thead>
<tr>
<th>Field</th>
<th>What to enter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>sys_user</td>
</tr>
<tr>
<td>Element</td>
<td>preferred_language</td>
</tr>
<tr>
<td>Language</td>
<td>Enter the two-character ISO 639.1 code for the language that the user is currently using before they select the new language. The default is <strong>en</strong>.</td>
</tr>
<tr>
<td>Label</td>
<td>Enter the name of the new language selection as you want it to appear in the language picker. For example, Mongolian.</td>
</tr>
<tr>
<td>Value</td>
<td>Enter the two-character ISO 639.1 code for the new language that the user is selecting. For example, <strong>mn</strong>.</td>
</tr>
<tr>
<td>Sequence</td>
<td>Enter a number to determine what order the option appears in the choice list if you do not want to list choices alphabetically. For example, <strong>5</strong>.</td>
</tr>
</tbody>
</table>

The following record allows a user who is using the Dutch localization of their instance to change languages to Mongolian:

- **Table**: User [sys_user]
- **Element**: preferred_language
- **Language**: nl
- **Label**: Mongoolse
- **Value**: mn

2. Export and translate those strings that you want to translate, as described in **Export and edit translation records**.
There is a very large number of translatable strings on the platform. Exporting all of them and translating them manually is probably not a realistic possibility. Consider exporting filtered subsets of the strings from each table and then translating them.

3. Import the translated document back into the instance as an import set, as described in Import a translation from an Excel spreadsheet.

Translating the knowledge base

The knowledge base has its own Translation Management system. When this is disabled, knowledge base articles use translated_html fields for translated content.

When any of the I18N internationalization plugins are enabled, the Knowledge Management Internationalization plugin is enabled. This plugin allows knowledge article authors to create language-specific articles and to translate and access articles. For more information about Knowledge Management internationalization, see Translation Management in the Knowledge Management documentation.

If the Knowledge Management Internationalization plugin is disabled, knowledge base articles use translated_html fields for article content. This type of field displays the translation based on the language of the user, if multiple translations are stored. To learn about using translated_html fields, see Translating text fields.

Translating Service Catalog cart labels

You can specify language-specific labels in these Service Catalog screens: Cart, Edit Cart, and Check Out (including workflows and approvals).

The text for the labels is stored on the Messages [sys_ui_message] table. Localized Message records for these labels are included in the I18N Internationalization language plugins. The application is Global. You can add a record for an unsupported language, or edit an existing record. If you edit an existing record, export the record to another application, edit it in that application, and re-import it. Otherwise, your edits may be overwritten when your instance is zbootted or updated. For more information about exporting translation records, see Export and edit translation records.
Localization Framework

ServiceNow Localization Framework standardizes and enhances the translation process of required artifacts such as ServiceNow® Service Catalog items and ServiceNow® Virtual Agent topics across the platform through configurable workflows.

Get started with Localization Framework

1. Procure any ServiceNow, Inc. subscription that is Standard or above.
3. Configure Localization Framework with the required artifacts. Service Catalog items and Virtual Agent topics are supported in the Quebec release. See Artifact configuration for more information.
4. Activate the required languages and configure them with Localization Framework. For more information, see Activate a language.

Activation of Localization Framework

When you activate the Localization Framework Installer plugin (com.glide.localization_framework.installer), Localization Framework is available by default for the Service Catalog items and Virtual Agent topics.

After you activate the Localization Framework Installer plugin (com.glide.localization_framework.installer), you can do the following tasks:
• Request translations of the artifacts into one or more languages.
• Translate artifacts using manual translation or any of the supported translation modes.
• Approve translations by proofreading the translated content.
• Publish the translated content.
• Analyze the localization health of the system using the Localization Insights dashboard.

For more information on activating this plugin, see Activate Localization Framework.

Activate Localization Framework

You can activate the Localization Framework Installer plugin (com.glide.localization_framework.installer) for Localization Framework if you have the admin role. The application installs related plugins if they are not already installed.

Role required: admin

The following items are installed with Localization Framework:
• Plugins
• Roles
• Scheduled jobs
• Tables

For more information, see Components installed with Localization Framework.

1. Navigate to System Applications > All Available Applications > All.
2. Find the Localization Framework Installer plugin (com.glide.localization_framework.installer) using the filter criteria and search bar.

You can search for the plugin by its name or ID. If you cannot find a plugin, you might have to request it from ServiceNow personnel. For more information, see Request a plugin.
3. Click Install, and then in the Activate Plugin dialog box, click Activate.

Note: When domain separation and delegated admin are enabled in an instance, the administrative user must be in the global domain. Otherwise, the following error appears: Application installation is unavailable because another operation is running: Plugin Activation for <plugin name>.

Components installed with Localization Framework

The Localization Framework Installer plugin (com.glide.localization_framework.installer) activates these related plugins that are not already active.

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Description</th>
</tr>
</thead>
</table>
## Localization Framework Roles

Localization Framework uses roles to manage different aspects of the application.

### Localization Framework Roles

<table>
<thead>
<tr>
<th>Role Title [Name]</th>
<th>Role Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Localization administrator [localization_admin]</td>
<td>Manages the following aspects of the Localization Framework application:</td>
</tr>
<tr>
<td></td>
<td>• Configures the supported artifacts and custom artifacts for Localization Framework.</td>
</tr>
<tr>
<td></td>
<td>• Configures localization settings for the activated languages.</td>
</tr>
<tr>
<td></td>
<td>• Can request translations into multiple languages for Service Catalog items, Virtual Agent topics, or for any custom artifacts from their respective artifact tables.</td>
</tr>
<tr>
<td></td>
<td>• Can request translations for Service Catalog items, Virtual Agent topics, or for any custom artifact for a particular language from their respective artifact reports in the insights dashboard.</td>
</tr>
<tr>
<td></td>
<td>• Can configure SDL and XTM TMS and can create and configure a custom TMS by inheriting the following roles:</td>
</tr>
<tr>
<td></td>
<td>• flow_designer: localization_admin with this role can edit the TMS subflows and can create a new TMS configuration record.</td>
</tr>
<tr>
<td></td>
<td>• connection_admin: localization_admin with this role can access the connections and credentials tables and records.</td>
</tr>
<tr>
<td></td>
<td>• Owns the localization insights dashboard and reports, and can execute the scheduled jobs to display the reports on the dashboard.</td>
</tr>
<tr>
<td></td>
<td>• Views the localization health of the system.</td>
</tr>
<tr>
<td></td>
<td>• localization_admin role inherits the localization_requester and localization_fulfiller roles.</td>
</tr>
<tr>
<td>Localization requester [localization_requester]</td>
<td>Requests translations for all the configured artifacts into one or more languages.</td>
</tr>
</tbody>
</table>
Role Title [Name] | Role Description
--- | ---
Localization fulfiller [localization_fulfiller] | Provides translations for the requested artifact items. Uses the following ways to translate the artifacts:
- Manual translation, if understands both the source and the target language.
- Machine translation, using the translator configured in the translation preferences.
- Exports data to a third-party translator and imports it back after translations.
- Sends the data via email for translations and receives the translated data back via email.
- Sends translatable data to a translation management system (TMS) for translations.
- Verifies and approves the translations.
- Publishes the translations if the language setting workflow has no approval flow.

Artifact configuration

You can configure the required artifacts and use the Localization Framework to fulfill the translation requests. Artifact configuration is a table where every configured artifact has its own record in the instance.

With the activation of the Localization Framework Installer plugin (com.glide.localization_framework.installer), a record for a service catalog item is automatically created and configured with the Localization Framework.

A record for the Virtual Agent topic is created and configured only with the activation of the Glide Virtual Agent plugin (com.glide.cs.chatbot). For more information on activating this plugin, see Activate Virtual Agent.

You can also create and configure an artifact of your choice and a record for the same is created in the Artifact Configuration [snLf_config] table. For more information, see Create and configure a custom artifact.

Create and configure a custom artifact

Create and configure custom artifacts of your choice to use the Localization Framework functionality.

Role required: localization_admin

Ensure you have activated the Localization Framework Installer plugin (com.glide.localization_framework.installer) before configuring a custom artifact of your choice.

1. Navigate to Localization Framework > Artifact Configuration.
2. Click New.
3. In the Artifact Configuration form, fill the fields.

Artifact Configuration form fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Identifier of the artifact record.</td>
</tr>
<tr>
<td>Table Name</td>
<td>Identifier of the table where information of the artifact is stored. For example, Catalog Items [sc_cat_item] table.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Read Script   | Extracts the translatable content associated with the translation request. The script is run each time a translation is requested and returns the translatable content of the artifact in a standardized JSON. Provide the following input and output read script contracts to configure the artifact:  

- Syntax of the input read script:

```javascript
(function(tableName, sysId, language) {
    // Code to generate document content json
})(table_name, sysId, language);
```

- JSON format of the output read script:

```json
{
    "version": "v1",
    "content": [
        {
            "groupName": "",
            "label": "",
            "fieldInfo": [
                {
                    "originalValue": "",
                    "translatedValue": ""
                }
            ]
        },
        {
            ...
        }
    ]
}
```
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save Script</td>
<td>Saves the translations into the database. The script is run each time the translation of an artifact is published.</td>
</tr>
<tr>
<td></td>
<td>Note:</td>
</tr>
<tr>
<td></td>
<td>• If the application uses one or more standard platform tables to store the translations, the save script is not required. For more information, see Translation tables.</td>
</tr>
<tr>
<td></td>
<td>• The save script is required when the application uses tables other than the standard tables to store the translations.</td>
</tr>
<tr>
<td></td>
<td>Provide the following save script contract to configure the artifact:</td>
</tr>
<tr>
<td></td>
<td>(function(taskId) { // Code to store translations of the localization task when the translations are published. })(taskId);</td>
</tr>
<tr>
<td>Application</td>
<td>Scope of the application. The value is Global by default.</td>
</tr>
<tr>
<td>Active</td>
<td>Option to activate the configuration record.</td>
</tr>
</tbody>
</table>

4. Click Submit.

**Create a UI action for the custom artifact**

Create a UI action to request translations for the custom artifact.

Role required: localization_admin

1. Navigate to the custom artifact table.
   Find the table using its table name. For example, [sys_cs_topic] is the table name for Virtual Agent topics.

2. Click the hamburger icon ( ) at any of the columns and navigate to ConfigureUI Actions.

3. Click New.

4. In the UI Actions form, fill in the fields.

**UI Action form fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name for the UI action. For example, Request Translations.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Client</td>
<td>Option to execute the script in the user's browser. When enabled, the <strong>Onclick</strong> field appears above the Condition field.</td>
</tr>
<tr>
<td>Condition</td>
<td>Name of the custom artifact table on which this UI action is being created.</td>
</tr>
<tr>
<td>Onclick</td>
<td>Provide the JavaScript function name as:</td>
</tr>
<tr>
<td></td>
<td><code>renderLanguagePickerModal();</code></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Script</td>
<td>Option to execute the script to run the request translations function. The script varies for <strong>Form button</strong> and <strong>List choice</strong>.</td>
</tr>
<tr>
<td>Form button</td>
<td>Option to enable the UI action as a form button.</td>
</tr>
</tbody>
</table>

**Form Button**

```javascript
function renderLanguagePickerModal() {
    var dlg = new GlideModal('sn_lf_language_picker');
    dlg.setTitle(getMessage('Request Translations'));
    dlg.setPreference('sys_id', g_form.getUniqueValue());
    dlg.setPreference('table_name', g_form.getTableName());
    dlg.setPreference('request_type', "form");
    dlg.render();
}
```

**List choice**

```javascript
function renderLanguagePickerModal() {
    var sys_ids = g_list.getChecked();
    if (!sys_ids || sys_ids.length == 0) return;
    var dlg = new GlideModal('sn_lf_language_picker');
    dlg.setTitle(getMessage('Request Translations'));
    dlg.setPreference('sys_id', sys_ids);
    dlg.setPreference('table_name', g_list.getTableName());
    dlg.setPreference('request_type', "list");
    dlg.render();
}
```
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>List choice</td>
<td>Option to enable the UI action in the choice list.</td>
</tr>
</tbody>
</table>

**Note:** Configure the form to see all the fields. For more information, see Create a UI action.

5. Click **Submit**.

**Read script helper functions for LFDocumentContentBuilder**

The *LFDocumentContentBuilder* provides utility functions to build document content JSON. These functions can be used while writing the read scripts only for artifacts that use standard tables for translation.

**initialize (version, targetLanguage)**

This function is a constructor for *LFDocumentContentBuilder* and includes the following parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>String</td>
<td>The version type of the document content to be generated. For Quebec, this value is v1.</td>
</tr>
<tr>
<td>targetLanguage</td>
<td>String</td>
<td>The target language of the localization task document content. The target language is the same as the language available from the read script function argument.</td>
</tr>
</tbody>
</table>

**processString (string, groupName, label)**

This function adds an entry in the document content for the given string and includes the following parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>string</td>
<td>String</td>
<td>The value for which a document content entry is created.</td>
</tr>
<tr>
<td>groupName</td>
<td>String</td>
<td>The group this string input belongs to.</td>
</tr>
<tr>
<td>label</td>
<td>String</td>
<td>The unique label identifier for this string input.</td>
</tr>
</tbody>
</table>

This function adds the following JSON object in document content:

```json
{
    'groupName': groupName,
    'label': label,
    'fieldInfo': [
        {
            "originalValue": string, translatedValue: <fetched from sys_ui_message table, if exists>}
    ]
}
```
**processStringArray (stringArray, groupName, label)**

This function adds an entry in the document content for the given string and includes the following parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>stringArray</td>
<td>List of Strings</td>
<td>The list of values for which document content entry is created.</td>
</tr>
<tr>
<td>groupName</td>
<td>String</td>
<td>The name of the group these strings belongs to.</td>
</tr>
<tr>
<td>label</td>
<td>String</td>
<td>The unique label identifier for these strings.</td>
</tr>
</tbody>
</table>

This function adds the following JSON object in document content:

```json
{
    'groupName': groupName,
    'label': label,
    'fieldInfo': [
        {
            "originalValue": string[0],
            "translatedValue": <fetched from sys_ui_message table, if exists>
        },
        {
            "originalValue": string[1],
            "translatedValue": <fetched from sys_ui_message table, if exists>
        },
        ...
    ]
}
```

**processScript (scriptContent, groupName, label)**

This function adds an entry in the document content for the strings present as input of `getMessage`, `gs.getMessage`, or `gs.getMessageLang` in the provided Script. It has the following parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scriptContent</td>
<td>String</td>
<td>The Script to be processed to get the strings present as input of <code>getMessage</code>, <code>gs.getMessage</code>, or <code>gs.getMessageLang</code>.</td>
</tr>
<tr>
<td>groupName</td>
<td>String</td>
<td>The name of the group for this input.</td>
</tr>
<tr>
<td>label</td>
<td>String</td>
<td>The unique label identifier for this input.</td>
</tr>
</tbody>
</table>

For example,

```javascript
var documentContentBuilder = new LFDocumentContentBuilder("v1", language);
var name = "name";
documentContentBuilder .processScript("gs.getMessage('Hello {0}, How are you', name)",
"Script_Group", "Script_Label");
```
This function adds the following JSON in document content:
{
    'groupName': "Script_Group",
    'label': label, "Script_Label"
    'fieldInfo': [
        {"originalValue": "Hello {0}, How are you", translatedValue: <fetched from sys_ui_message table, if exists>},
        ...
    ]
}

**processTranslatableFieldsForSingleRecord (glideRecord, groupName)**

This function creates entries for the given glideRecord object, in document content for all its translatable fields. These translatable fields can be of translated_field, translated_text or translated_html types. It includes the following parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glideRecord</td>
<td>GlideRecord</td>
<td>The GlideRecord object to be processed for translatable fields. The GlideRecord should be pointing to the valid table record.</td>
</tr>
<tr>
<td>groupName</td>
<td>String</td>
<td>The name of the group for this input.</td>
</tr>
</tbody>
</table>

**processTranslatableFieldsForMultipleRecords (tableName, encodedQuery, groupName)**

This function fetches all the qualified records for the given tableName and encodedQuery and adds entries in the document content for all the translatable fields. It includes the following parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tableName</td>
<td>String</td>
<td>The table to fetch records.</td>
</tr>
<tr>
<td>encodedQuery</td>
<td>String</td>
<td>The encoded query for filtering records from the processTranslatableFieldsForSingleRecord table.</td>
</tr>
<tr>
<td>groupName</td>
<td>String</td>
<td>The name of the group for this input.</td>
</tr>
</tbody>
</table>

**getFinalJSON**

Returns the final built document content JSON.

**Localization Framework Settings**

You can define translation and workflow preferences for one or more activated languages with Localization Framework Settings.

Before you define the translation and workflow preferences, ensure to activate all the required languages in the instance to define the localization preferences. For more information, see [Activate a language](#).
You must configure at least one of the following translation modes to define the translation preferences. For more information, see Translation modes.

- Activate the required translator if you want to use machine translation.

  **Note:** Machine translation in the Localization Framework is powered by Dynamic Translation.

- Configure a TMS service of your choice if you want to send the content to a translation management system for translation. For more information, see Translation Management System configuration.

- Configure an email subflow if you want to use a subflow other than the default subflow for sending the translatable content file for translation via email. For more information, see Create a custom email subflow.

  **Note:** You cannot define the translation preferences for a language without enabling at least one of the translation modes.

### Create a custom email subflow

Create an email subflow according to your requirements. You can then select this subflow to define translation preferences for a language.

Roles required: localization_admin and flow_designer

The Localization Framework provides a default email subflow that you can customize.

Copy the existing email subflow configured for the Localization Framework and then customize it. Publish the customized subflow so that it is available for selection when setting up the translation preference for a language. For more information, see Create a subflow.

1. Navigate to **Process Automation > Flow Designer**.
2. In the Flow Designer window, click **Subflows**.
3. Click **Send LF Email for Translation** subflow.

   The Send LF Email for Translation subflow opens in the Flow Designer in read-only format. The inputs in this subflow are described in the following table:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>attachment_record</td>
<td>Contains a file related to the LFTASK that can be sent via Email for translation.</td>
<td>Reference.Attachment</td>
</tr>
<tr>
<td>send_to</td>
<td>Contains email addresses of the recipients to send the LF task file.</td>
<td>String</td>
</tr>
<tr>
<td>source_language</td>
<td>Language from which the localization task was created.</td>
<td>String</td>
</tr>
<tr>
<td>target_language</td>
<td>Language into which the content of the localization task gets translated into.</td>
<td>String</td>
</tr>
</tbody>
</table>
4. In the subflow header, click the more actions icon and select **Copy subflow**.

5. In the **New subflow name** field, enter the name of the new subflow.

6. To limit the application scope of the subflow, in the **Application** field, select the required application, otherwise select **Global**.

7. Click **Copy**.

The new subflow is created and opens in the subflow designer editor. The inputs from the copied subflow appear.

**Note:** Inputs are fixed and cannot be edited.

8. In the Actions section, click **Send Email**.

This expands the Send Email section. The fields in the Send Email section are described below:

<table>
<thead>
<tr>
<th>Field name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Name of the action.</td>
</tr>
<tr>
<td></td>
<td>Default: <strong>Send Email</strong></td>
</tr>
<tr>
<td>Target Record</td>
<td>Associated Localization Framework task record</td>
</tr>
<tr>
<td>Table</td>
<td>Name of the table where the localization task resides.</td>
</tr>
<tr>
<td>Include Watermark</td>
<td>Adds a watermark in the file associated with the</td>
</tr>
<tr>
<td></td>
<td>localization task.</td>
</tr>
<tr>
<td>To</td>
<td>Contains email addresses of the recipients who should</td>
</tr>
<tr>
<td></td>
<td>be addressed directly.</td>
</tr>
<tr>
<td>CC</td>
<td>Contains email addresses of the recipients who should</td>
</tr>
<tr>
<td></td>
<td>see the list of recipients directly addressed in the</td>
</tr>
<tr>
<td></td>
<td>email.</td>
</tr>
<tr>
<td>BCC</td>
<td>Contains email addresses of the recipients who are</td>
</tr>
<tr>
<td></td>
<td>copied on the email but not displayed in the email.</td>
</tr>
<tr>
<td>Subject</td>
<td>The text about the email that its recipients can see.</td>
</tr>
<tr>
<td>Body</td>
<td>The text message about the localization task being</td>
</tr>
<tr>
<td></td>
<td>sent for translation.</td>
</tr>
</tbody>
</table>

9. Click **Done**, when you have modified the fields as per your requirement.

10. Click **Copy Attachment**.

The Copy Attachment action expands. The fields in the Copy Attachment section are described below:

<table>
<thead>
<tr>
<th>Field name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Name of the action.</td>
</tr>
<tr>
<td></td>
<td>Copy Attachment is displayed by default.</td>
</tr>
<tr>
<td>Source Attachment Record [Attachment]</td>
<td>Translatable content file of the localization task.</td>
</tr>
<tr>
<td>Field name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Target Record</td>
<td>Represents the target record in the email.</td>
</tr>
<tr>
<td>Table</td>
<td>Represents the email table.</td>
</tr>
</tbody>
</table>

11. Click **Save**, to save the subflow in draft status.
12. Click **Publish**.

Use the published subflow to define the translation preference for a language.

**Translation Management System configuration**

The Localization Framework supports integration with a translation management system to localize the content. The TMS configuration table lists all the TMS services configured in the instance.

By default, SDL TMS and XTM TMS services are supported in Localization Framework with the activation of the Localization Framework Installer plugin (com.glide.localization_framework.installer) and appear in the TMS configuration [sn_lf_tms_config] table.

To use SDL TMS service for localization of the artifacts, you need to configure the connection and credentials. For more information about configuring SDL TMS, see **SDL Translation Management System spoke**.

To use XTM TMS service for localization of the artifacts, you need to configure the connection and credentials. For more information about configuring XTM TMS, see **XTM Translation Management System spoke**.

You can also sign up and create an account with a TMS service of your choice. To create and configure a custom TMS, see **Create a custom translation management system**.

**SDL Translation Management System spoke**

The SDL Translation Management System spoke provides subflows and actions to localize the artifacts using the SDL translation management system service.


**Subscription**

The SDL TMS spoke requires any ServiceNow subscription that is Standard or above and includes the Localization Framework.

**Supported versions**

Version v1

**Spoke Subflows**

The spoke provides subflows in the Published state to integrate with the SDL TMS service. These subflows can be used as part of other subflows and flows.
Spoke subflows

<table>
<thead>
<tr>
<th>Subflow</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request Translations [request_translations]</td>
<td>Contains set of inputs and outputs to request translations of the artifacts.</td>
</tr>
<tr>
<td>Retrieve Translations [retrieve_translations]</td>
<td>Contains set of inputs and outputs to retrieve translations of the translated artifacts.</td>
</tr>
</tbody>
</table>

Spoke actions

The spoke provides actions to integrate with the SDL TMS service.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Project [create_project_on_sdl]</td>
<td>Creates a project on SDL for translation.</td>
</tr>
<tr>
<td>Get Project Details [get_sdl_project_details]</td>
<td>Fetches the project's details for the translation request.</td>
</tr>
<tr>
<td>Get Translated File [get_translated_file_from_sdl]</td>
<td>Fetches the translated file from SDL TMS after translations.</td>
</tr>
<tr>
<td>Mark File As Complete [complete_file_on_sdl]</td>
<td>Marks the file as complete, after getting the translated content.</td>
</tr>
</tbody>
</table>

SDL Translation Management System account requirements

Ensure that you are registered with SDL TMS and obtain the credential information. For more information on SDL Managed Translation API, see SDL documentation.

Connection and Credential alias requirements

The IntegrationHub uses aliases to manage connection and credential information. Using an alias eliminates the need to configure multiple credentials and connection information profiles when using multiple environments. If the connection or credential information changes, you do not need to update any actions that use the connection. For more information, see Connections and Credentials Information.

To use the spoke connection aliases, use an associated connection record and a credential record created with the SDL spoke installation.

This spoke uses the SDL TMS alias (sn_sdl_speak.SDL_TMS) to authorize actions.

- Connection alias requirements
  - Connection type: HTTP
  - Connection URL: For example, https://languagecloud.sdl.com. This is a sample URL. Users can have a different URL based on their geographical preference.

See Configure SDL TMS in the Localization Framework to connect to the SDL TMS services and use them to localize the artifacts.
Configure SDL TMS in the Localization Framework

Configure SDL TMS to use the SDL TMS service in the Localization Framework.

Roles required: connection_admin

1. Navigate to Connections & Credentials > Connection & Credential Aliases.
   A credential record for SDL TMS is created when the SDL TMS spoke is installed with the Localization Framework Installer plugin (com.glide.localization_framework.installer) activation.

2. Open the SDL TMS credential record.
3. In the Connections related list, open the SDL connection record.
   A connection record for SDL is created when the SDL TMS spoke is installed with the Localization Framework Installer plugin (com.glide.localization_framework.installer) activation.
   All the form fields are populated with the information that is fetched through the SDL spoke installation during the Localization Framework Installer plugin (com.glide.localization_framework.installer) activation.

4. In the Attributes section of the HTTP(s) Connection form, provide the project_option_id connection attribute, and save the form.
   SDL provides an option to create automated or reviewed projects and provides the respective option IDs during SDL account creation.

5. In the Credential field, click the information icon
   and open the record.
   A record for OAuth 2.0 credentials is created when the SDL TMS spoke is installed with the Localization Framework Installer plugin (com.glide.localization_framework.installer) activation.

6. In the OAuth Entity Profile field, click the information icon
   and open the record.
   An OAuth Entity profile is created when the SDL TMS spoke is installed with the Localization Framework Installer plugin (com.glide.localization_framework.installer) activation.

7. In the OAuth provider field, click the information icon
   and open the record.
   An Application Registries record is created when the SDL TMS spoke is installed with the Localization Framework Installer plugin (com.glide.localization_framework.installer) activation.

8. Provide the Client ID and Client Secret provided by SDL at the time of account creation, and save the form.
9. Open the OAuth 2.0 Credentials form again, and click the Get OAuth Token related link.
10. Provide the username and password.
    SDL supports resource owner password credentials as the grant type. Provide these credentials to generate the token for the first time.

   **Note:** The username and password do not persist in the ServiceNow instance.

11. Click Get OAuth Token.
    Once the OAuth token is created, the ServiceNow® platform regenerates the token until the refresh token expires.
XTM Translation Management System spoke

The XTM Translation Management System spoke provides subflows and actions to localize the artifacts using the XTM translation management system service.


Subscription

The XTM TMS spoke requires any ServiceNow subscription that is Standard or above and includes the Localization Framework.

Supported versions

Version v1

Spoke Subflows

The spoke provides subflows in the Published state to integrate with the XTM TMS service. These subflows can be used as part of other subflows and flows.

Spoke subflows

<table>
<thead>
<tr>
<th>Subflow</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request Translations</td>
<td>Contains set of inputs and outputs to request translations of the artifacts.</td>
</tr>
<tr>
<td>Retrieve Translations</td>
<td>Contains set of inputs and outputs to retrieve translations of the translated artifacts.</td>
</tr>
</tbody>
</table>

Spoke actions

The spoke provides actions to integrate with the XTM TMS service.

Spoke actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Project</td>
<td>Creates a project on XTM for translation.</td>
</tr>
<tr>
<td>Get Project Details</td>
<td>Fetches the project's details for the translation request.</td>
</tr>
<tr>
<td>Get Translated File</td>
<td>Fetches the translated file from XTM TMS after translations.</td>
</tr>
</tbody>
</table>
XTM Translation Management System account requirements

Ensure that you are registered with XTM TMS and obtain the credential information. For more information, see XTM documentation.

Connection and Credential alias requirements

The IntegrationHub uses aliases to manage connection and credential information. Using an alias eliminates the need to configure multiple credentials and connection information profiles when using multiple environments. If the connection or credential information changes, you do not need to update any actions that use the connection. For more information, see Connections and Credentials Information.

To use the spoke connection aliases, use an associated connection record and a credential record created with the XTM TMS spoke installation.

This spoke uses the XTM TMS alias (sn_xtm_spoke.XTM_TMS) to authorize actions.

- Connection alias requirements
  - Connection type: HTTP
  - Connection URL: For example, https://api-test.xtm-intl.com. This is a sample URL. Users can have a different URL based on their geographical preference.

See Configure XTM TMS in the Localization Framework to connect to the XTM TMS services and use them to localize the artifacts.

Configure XTM TMS in the Localization Framework

Configure XTM TMS to use the XTM TMS service in the Localization Framework.

Roles required: connection_admin

1. Navigate to Connections & Credentials > Connection & Credential Aliases. A credential record for XTM TMS is created when the XTM TMS spoke is installed with the Localization Framework Installer plugin (com.glide.localization_framework.installer) activation.
2. Open the XTM TMS credential record.
3. In the Connections related list, open the XTM connection record. A connection record for XTM is created when the XTM TMS spoke is installed with the Localization Framework Installer plugin (com.glide.localization_framework.installer) activation.
   All the form fields are populated with the information fetched through the XTM spoke installation during the Localization Framework Installer plugin (com.glide.localization_framework.installer) activation.
4. In the Attributes section of the HTTP(s) Connection form, provide the *template_id* and *customer_id* connection attributes, and save the form.
5. In the Credential field, click the information icon and open the record. A record for OAuth 2.0 credentials is created when the XTM TMS spoke is installed with the Localization Framework Installer plugin (com.glide.localization_framework.installer) activation.
6. In the OAuth Entity Profile field, click the information icon and open the record. An OAuth Entity Profile is created when the XTM TMS spoke is installed with the Localization Framework Installer plugin (com.glide.localization_framework.installer) activation.
7. In the **OAuth provider** field, click the information icon

![information icon](image)

and open the record.

An Application Registries record is created when the XTM TMS spoke is installed with the Localization Framework Installer plugin (com.glide.localization_framework.installer) activation.

8. Provide the Client ID and Client Secret provided by XTM at the time of account creation, and save the form.

9. Open the OAuth 2.0 Credentials form again, and click the **Get OAuth Token** related link.

10. Provide the username and password.

    XTM supports resource owner password credentials as the grant type. Provide these credentials to generate the token for the first time.

    **Note:** The username and password do not persist in the ServiceNow instance.

11. Click **Get OAuth Token**.

    Once the OAuth token is created, the ServiceNow® platform regenerates the token until the refresh token expires.

---

**Integrate with a translation management system**

Integrate with any translation management system of your choice to localize the artifacts requested for translations.

Role required: localization_admin

1. Create subflows to request translations and to retrieve the translated content. Use IntegrationHub subflows, actions, and connections and credentials.

   a) Ensure that the error messages and codes from the TMS provider are mapped correctly with the error messages and codes supported the ServiceNow platform.

   **Standard error codes and messages**

<table>
<thead>
<tr>
<th>Error code</th>
<th>Error message</th>
</tr>
</thead>
<tbody>
<tr>
<td>40510</td>
<td>Error while requesting translations.</td>
</tr>
<tr>
<td>40520</td>
<td>Error while retrieving translations.</td>
</tr>
<tr>
<td>40500</td>
<td>Authentication failed.</td>
</tr>
</tbody>
</table>

   b) Ensure that the input and output fields are in the following format for the subflows:

   **Request translation subflow**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>lftask_number</td>
<td>Associated localization task number.</td>
<td>String</td>
</tr>
<tr>
<td>xliff_1_2_content</td>
<td>Content of an artifact which must be translated in XLIFF 1.2 format. For example,</td>
<td>String</td>
</tr>
<tr>
<td></td>
<td>'csv', 'xliff 1.2'</td>
<td></td>
</tr>
</tbody>
</table>
### ServiceNow

#### DocVersion

Now Platform administration

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inputs</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>source_language</td>
<td>Language code of the source text. For example, 'en'</td>
<td>String</td>
</tr>
<tr>
<td>target_language</td>
<td>Language code of the target text. For example, 'fr', 'it'</td>
<td>String</td>
</tr>
<tr>
<td><strong>Outputs</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>project_info</td>
<td>The ID for the project created for an artifact configuration.</td>
<td>Object</td>
</tr>
<tr>
<td>status</td>
<td>Status of the request. For example, Success or Failure.</td>
<td>Choice</td>
</tr>
<tr>
<td>error_message</td>
<td>The reason for the error that populates when an error occurs.</td>
<td>String</td>
</tr>
<tr>
<td>error_code</td>
<td>The error code that populates when an error occurs.</td>
<td>String</td>
</tr>
</tbody>
</table>

**Retrieve translation subflow**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inputs</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>lftask_number</td>
<td>Associated localization task number.</td>
<td>String</td>
</tr>
<tr>
<td>project_info</td>
<td>The ID for the project created for an artifact configuration.</td>
<td>Object</td>
</tr>
<tr>
<td><strong>Outputs</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>translated_xliff_1_2</td>
<td>Translated XLIFF file received from the TMS.</td>
<td>String</td>
</tr>
<tr>
<td>status</td>
<td>Status of the request. For example, Success or Failure.</td>
<td>Choice</td>
</tr>
<tr>
<td>error_message</td>
<td>The reason for the error that populates when an error occurs.</td>
<td>String</td>
</tr>
<tr>
<td>error_code</td>
<td>The error code that populates when an error occurs.</td>
<td>String</td>
</tr>
</tbody>
</table>
2. Create and configure a custom translation management system and activate it. See Create a custom translation management system.

**Note:** Localization Framework depends on IntegrationHub to build integrations with third-party systems.

### Create a custom translation management system

Configure Localization Framework with a third-party translation management system of your choice to localize an artifact.

Roles required: localization_admin and flow_designer

Ensure that the Localization Framework Installer plugin (com.glide.localization_framework.installer) is activated.

1. Navigate to **Localization Framework > TMS Configuration**.

**Note:** By default, SDL and XTM translation management system configurations are available.

2. Click **New**.

3. In the TMS Configuration form, fill in the fields.

#### TMS Configuration form fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Identifier of the TMS configuration.</td>
</tr>
<tr>
<td>Request Translation Subflow</td>
<td>IntegrationHub subflow that interacts with the third-party translation management system to request translations.</td>
</tr>
<tr>
<td>Retrieve Translation Subflow</td>
<td>IntegrationHub subflow that interacts with the third-party translation management system to retrieve translated content.</td>
</tr>
<tr>
<td>Application</td>
<td>The scope of the application. The default value is Global.</td>
</tr>
<tr>
<td>Version</td>
<td>Version of the contract used in subflows. The default value is v1.</td>
</tr>
<tr>
<td>Enable auto retrieval</td>
<td>Option to retrieve the translated content automatically. When selected, the translations are retrieved as per the scheduled jobs which runs daily.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

### Define Translation and Workflow Preferences

Define translation and workflow preferences for one or more activated languages to request translations in Localization Framework.

Role required: localization_admin

1. Navigate to **Localization Framework > Settings**.

2. Click **New**.
3. On the form, fill the fields.

**Settings form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Identifier of the translation settings.</td>
</tr>
<tr>
<td>Languages</td>
<td>Target records of the activated languages.</td>
</tr>
<tr>
<td>Application</td>
<td>Scope of the application. The default application scope is Global.</td>
</tr>
</tbody>
</table>

*Note:* Ensure to activate the languages before setting up the translation preferences and select one or more languages from the list.

4. Click the **Translation Preferences** tab and fill the fields.

**Translation Preferences form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Machine Translate</strong></td>
<td></td>
</tr>
<tr>
<td>Enable Machine Translate</td>
<td>Option to enable machine translation service for one or more selected languages.</td>
</tr>
<tr>
<td></td>
<td><em>Note:</em> Ensure that you install Dynamic Translation to use machine translation. For more information, see Activate Dynamic Translation.</td>
</tr>
<tr>
<td>Translator</td>
<td>Select a translator of your choice for machine translation.</td>
</tr>
<tr>
<td></td>
<td><em>Note:</em> Ensure that the corresponding translator configuration record is active and contains a translation subflow of version v3.</td>
</tr>
<tr>
<td><strong>Translation Management System</strong></td>
<td></td>
</tr>
<tr>
<td>Enable TMS</td>
<td>Option to enable Translation Management System for one or more selected languages.</td>
</tr>
<tr>
<td>TMS</td>
<td>Select a TMS service of your choice. By default, the SDL and the XTM TMS are available. You can also choose a configured custom TMS. For more information, see Create and configure a custom artifact.</td>
</tr>
<tr>
<td><strong>Send via Email</strong></td>
<td></td>
</tr>
<tr>
<td>Enable Send via Email</td>
<td>Option to enable email service for content localization for one or more selected languages.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Email Subflow</td>
<td>Select a subflow for your email.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> A subflow exists by default. If you want to choose another subflow, ensure that you've created the subflow before setting up the translation preference.</td>
</tr>
<tr>
<td>Default File Format</td>
<td>Select a file format to send and receive the content. By default, XLIFF 1.2 and CSV file formats are supported.</td>
</tr>
<tr>
<td>Default Recipients List</td>
<td>Provide the required recipient email addresses in the translation preferences for one or more selected languages to send an email.</td>
</tr>
<tr>
<td>Export/Import</td>
<td>Option to enable the export and import of content for translation for one or more selected languages.</td>
</tr>
<tr>
<td>Default File Format</td>
<td>Select a file format to send and receive the content. By default, XLIFF 1.2 and CSV file formats are supported.</td>
</tr>
</tbody>
</table>

5. Click the **Workflow Preferences** tab and fill the fields.

**Workflow Preferences form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workflow</td>
<td>Select a workflow for translations in one or more selected languages.</td>
</tr>
<tr>
<td></td>
<td><strong>For more information on the available workflows, see Workflows in the Localization Framework.</strong></td>
</tr>
<tr>
<td>Business Approver Group</td>
<td>Select the required business approver group from the available groups.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Ensure that the business approver group contains the localization_fulfiller role.</td>
</tr>
<tr>
<td>Localization Fulfiller Group</td>
<td>Select the required localization fulfiller group from the available groups.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Ensure that the localization fulfiller group contains the localization_fulfiller role.</td>
</tr>
<tr>
<td>Auto Translation Mode</td>
<td>Select the required auto-translation mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Machine Translate, Send to TMS, and Send via Email</strong> are the available options.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Ensure that you've configured the Translation Preferences for the selected auto translation mode.</td>
</tr>
</tbody>
</table>
6. Click **Submit**.

### Workflows in the Localization Framework

Workflows define actions for completing a localization task. Each localization task undergoes the workflow configured for its target language to complete the task.

<table>
<thead>
<tr>
<th>Workflows</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Translation # Publish</td>
<td>The localization task undergoes translation manually or by using one of the translation modes. After translation, the content gets published manually.</td>
</tr>
<tr>
<td>Translation # Approval of Translations # Auto Publish</td>
<td>The localization task undergoes translation manually or by using one of the translation modes. After translation, the task undergoes translation approval and gets auto-published.</td>
</tr>
<tr>
<td>Auto Translation # Approval of Translations # Auto Publish</td>
<td>The localization task undergoes auto-translation. After translation, the task undergoes translation approval and gets auto-published.</td>
</tr>
<tr>
<td>Auto Translation # Publish</td>
<td>The localization task undergoes auto-translation and gets published manually.</td>
</tr>
</tbody>
</table>

**Note:** Ensure that you assign the **Localization Fulfiller Group** and **Translation Approver Group** for the workflow to localize the content.
<table>
<thead>
<tr>
<th>Workflows</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Auto Translation # Auto Publish</strong></td>
<td>The localization task undergoes auto-translation and gets auto-published.</td>
</tr>
<tr>
<td><strong>Note:</strong> Ensure that you assign the <strong>Localization Fulfiller Group</strong> and <strong>Auto Translation Mode</strong> for the workflow to localize the content.</td>
<td></td>
</tr>
<tr>
<td><strong>Business Approval # Translation # Publish</strong></td>
<td>The localization task needs business approval for localization. The content gets translated manually or translated by using one of the translation modes. The content gets manually published.</td>
</tr>
<tr>
<td><strong>Note:</strong> Ensure that you assign the <strong>Business Approver Group</strong> and <strong>Localization Fulfiller Group</strong> for the workflow to localize the content.</td>
<td></td>
</tr>
<tr>
<td><strong>Business Approval # Translation # Approval of Translations # Auto Publish</strong></td>
<td>The localization task needs business approval for localization, and the content gets translated manually or by using one of the translation modes. After translation, the task undergoes translation approval and gets auto-published.</td>
</tr>
<tr>
<td><strong>Note:</strong> Ensure that you assign the <strong>Business Approver Group</strong>, <strong>Localization Fulfiller Group</strong>, and <strong>Translation Approver Group</strong> for the workflow to localize the content.</td>
<td></td>
</tr>
<tr>
<td><strong>Business Approval # Auto Translation # Approval of Translations # Auto Publish</strong></td>
<td>The localization task needs business approval for localization, and the content gets auto-translated. After translation, the task undergoes translation approval and gets auto-published.</td>
</tr>
<tr>
<td><strong>Note:</strong> Ensure that you assign the <strong>Business Approver Group</strong>, <strong>Localization Fulfiller Group</strong>, <strong>Auto Translation Mode</strong>, and <strong>Translation Approver Group</strong> for the workflow to localize the content.</td>
<td></td>
</tr>
<tr>
<td><strong>Business Approval # Auto Translation # Publish</strong></td>
<td>The localization task needs business approval for localization. The content gets auto-translated but gets manually published.</td>
</tr>
<tr>
<td><strong>Note:</strong> Ensure that you assign the <strong>Business Approver Group</strong>, <strong>Localization Fulfiller Group</strong>, and <strong>Auto Translation Mode</strong> for the workflow to localize the content.</td>
<td></td>
</tr>
<tr>
<td>Workflows</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Business Approval # Auto Translation # Auto Publish</td>
<td>The localization task needs business approval for localization. The content gets auto-translated and auto-published.</td>
</tr>
</tbody>
</table>

**Note:** Ensure that you assign the **Business Approver Group, Localization Fulfiller Group, and Auto Translation Mode** for the workflow to localize the content.

---

**Request Translations UI**

The Localization Framework enables you to select one or more activated languages while requesting translations for artifacts.

**Request Translations UI in the Localization Framework**

- Needs localization preferences to be defined for activated languages to request translations.

**Note:** Languages without localization settings are disabled for selection while requesting translations.

- Lists all the activated languages in the instance to choose for localization of the content.
- Displays the translations status of the artifacts in each of the activated languages based on the generated insights dashboard reports.
- Enables you to request translations for artifacts into one or more activated languages from their artifact tables.

Request Translations

Choose languages to translate into. Learn more

- Chinese *not translated*
- Dutch *not translated*
- French *completely translated*
- German *translation in progress*
- Telugu *not translated*
- Brazilian Portuguese *not translated*
- French - Canada *not translated*

Translation status last updated on 2020-12-01.

Cancel  Submit

Request translations UI from an artifact table
Enables you to request translations in the selected language from the localization dashboard for the selected insights records.

Request translations from the Insights list view

**Request translations for a Service Catalog item**

Request translations for a single Service Catalog item to localize it into one or more languages.

Roles required:
- localization_requester: To request translations
- catalog_editor: To access the Service Catalog items [sc_cat_item] table.

1. Navigate to **Service Catalog > Catalog Definitions > Maintain Items**.
2. Open a catalog item.
3. Click **Request Translations** on the form header.
4. Select the languages.
5. Click **Submit**.
   
   A localization task is created for each selected language.

**Request translations for multiple Service Catalog items**

Request translations for multiple Service Catalog items to localize them into one or more languages.

Roles required:
- localization_requester: To request translations
- catalog_editor: To access the Service Catalog items [sc_cat_item] table.

1. Navigate to **Service Catalog > Catalog Definitions > Maintain Items**.
2. Select multiple items from the list or select the **Select All** check box.
3. From the **Actions on selected rows** list, select **Request Translations**.
4. Select the languages.
5. Click **Submit**.

   Localization tasks are created for the selected items in all the selected languages.
Request translations for a Virtual Agent topic

Request translations for a Virtual Agent topic to localize it into one or more languages.

Roles required:

- localization_requester: To request translations.
- virtual_agent_admin: To access the Virtual Agent topics [sys_cs_topic] table.

1. Navigate to the Virtual Agent topics [sys_cs_topic] table.
2. Open a published topic.
3. Click Request Translations on the form header.
4. Select languages for translation.
5. Click Submit.

A localization task is created for each selected language.

Request translations for multiple Virtual Agent topics

Request translations for multiple Virtual Agent topics to localize them into one or more languages.

Roles required:

- localization_requester: To request translations.
- virtual_agent_admin: To access the Virtual Agent topics [sys_cs_topic] table.

1. Navigate to the Virtual Agent topics [sys_cs_topic] table.
2. Select multiple topics from the list or select the Select All check box.
3. From the Actions on selected rows list, select Request Translations.
4. Select the languages.
5. Click Submit.

Localization tasks are created for the selected topics in all the selected languages.

Localization task states

The state of a localization task defines the status of the localization request. The states of the localization tasks change based on the workflow defined for the language into which translations are requested.

<table>
<thead>
<tr>
<th>Task States</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awaiting Business Approval</td>
<td>The localization task is awaiting business approval.</td>
</tr>
<tr>
<td>Awaiting Translation</td>
<td>The localization task is waiting for translation by a localization fulfiller.</td>
</tr>
<tr>
<td>Translation in Progress</td>
<td>The localization task is undergoing translation.</td>
</tr>
<tr>
<td>Error in Translation</td>
<td>The localization task has encountered an error while translating the content.</td>
</tr>
<tr>
<td>Translations Approved</td>
<td>The localization task has been approved after translation.</td>
</tr>
</tbody>
</table>
## State

<table>
<thead>
<tr>
<th>State</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awaiting Translation Approval</td>
<td>The localization task needs translation approval to publish. The translation approver verifies the translations and approves the translations or requests the translator to review the translations.</td>
</tr>
<tr>
<td>Closed Complete</td>
<td>The localization task has been fulfilled and the translations are published.</td>
</tr>
<tr>
<td>Error in Publishing Translations</td>
<td>The localization task has encountered an error while publishing the translations.</td>
</tr>
<tr>
<td>Closed Incomplete</td>
<td>The localization task has been closed without fulfilling the request.</td>
</tr>
</tbody>
</table>

### Translation modes

The Localization Framework offers various translation modes for content translation. Localization fulfiller can use one of the translation modes to translate the content and fulfill the localization request.

#### Machine Translate

Machine translation in the Localization Framework is powered by the Dynamic Translation.

Activate the required translation service provider in the instance to machine translate the content. For information, see Create a translator configuration.

#### Send to TMS

The Localization Framework integrates with third-party Translation Management Systems to localize the content. SDL and XTM Translation Management Systems are supported by default and requires configuration. For more information see, Configure SDL TMS in the Localization Framework and Configure XTM TMS in the Localization Framework.

You can configure a custom Translation Management System of your choice. For more information, see Create a custom translation management system.

#### Send via Email

The Localization Framework provides Send via Email as a translation mode which can be used to send the translatable content for translation to a TMS service via email.

You can configure the Send via Email mode as a translation preference for one or more activated languages. For more information see, Define Translation and Workflow Preferences.

### Fulfill a localization task

Fulfill a localization task created for each selected language in the translation request.

Role required: localization_fulfiller

2. Open a localization task with the state **Awaiting Translation**, **Translation in Progress** or **Error in Translation**.

3. Click **Translate** in the form header.

   • The **Translate** UI action is available only for localization tasks created for languages with the following workflow preferences:
     • Translation # Publish
     • Translation # Approval of Translations # Auto Publish
     • Business Approval # Translation # Publish
     • Business Approval # Translation # Approval of Translations # Auto Publish

   The form turns into a two-column comparison layout with **Source Language** column on the left and **Target Language** column on the right.

4. Translate the content manually or select one of the following translation modes from the task header:

<table>
<thead>
<tr>
<th>Translation Mode</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Machine Translate</strong></td>
<td>Translates content using the translation service provider configured in the translation preferences.</td>
</tr>
<tr>
<td><strong>Send to TMS</strong></td>
<td>Sends the artifact to the translation management system configured in translation preferences for translation.</td>
</tr>
<tr>
<td><strong>Export Source File</strong></td>
<td>Exports the source file in the file format configured in translation preferences for translation.</td>
</tr>
<tr>
<td><strong>Send Source File via Email</strong></td>
<td>Sends the source file to the email addresses configured in translation preferences for translation.</td>
</tr>
</tbody>
</table>

5. Optional: Click the **Lock** icon beside the field with verified translations only if you want to make any changes to the verified translations. Verified translations are pre-existing translations available in the database for the given text. The framework automatically fetches the existing translations and locks the fields.

6. Optional: Click **Save as Draft** to save the translated content and revisit later or to send for translation approval. This option moves the task state to **Translation in Progress**

7. Click **Submit for Approval**.

   **Note:** This option is available only for tasks where the workflow configured for the target language needs translation approval.

   The task is sent for translation approval.

8. Click **Publish Translations**.

   **Note:** This option is available only for tasks where the workflow configured for the target language has the **Publish** option.

   The translations of the localization task are published and the task is updated with **Closed Complete** state.
Approve a localization task

Proofread the translated content and approve a localization task.

Role required: localization_fulfiller

2. Open a localization task with the state Awaiting Translation Approval.
3. Click Verify Translations.
4. Proofread the translations.
5. If the translations need a review, click Request Changes.
6. Click Approve to approve and publish the translations.

Error messages in the Localization Framework

Error messages are displayed when the appropriate settings are not configured for the translation and workflow preferences.

**Error messages in Settings**

<table>
<thead>
<tr>
<th>Error message</th>
<th>Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contains invalid Email Address(es):</td>
<td>When some of the email addresses fail the validation.</td>
</tr>
<tr>
<td>Enable at least one of the translation preferences.</td>
<td>When no translation preference is selected in the setting record.</td>
</tr>
<tr>
<td>Selected Localization Fulfiller group does not have the required role(s).</td>
<td>When the selected user group does not have the lf_fulfiller role.</td>
</tr>
<tr>
<td>Selected business approver group does not have the required role(s).</td>
<td>When the selected user group doesn’t have the lf_fulfiller role.</td>
</tr>
<tr>
<td>Selected Translation Approver group does not have the required role(s).</td>
<td>When the selected user group does not have the lf_fulfiller role.</td>
</tr>
<tr>
<td>Ensure the corresponding translation preference for your auto translation option is enabled.</td>
<td>When auto translate is selected in the workflow preference.</td>
</tr>
<tr>
<td>Selected Translator is not of version v3.</td>
<td>When the corresponding translator version is not v3.</td>
</tr>
<tr>
<td>Selected translator has no translate subflow configured.</td>
<td>When the corresponding translator's translate subflow is empty.</td>
</tr>
<tr>
<td>Selected translator is not active.</td>
<td>When the corresponding translator configuration is inactive.</td>
</tr>
<tr>
<td>A setting record already exists for the language(s): {0}.</td>
<td>When one or more selected languages are already part of another setting's record.</td>
</tr>
</tbody>
</table>

**Error messages in Request Translations**

<table>
<thead>
<tr>
<th>Error message</th>
<th>Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your request for translations failed.</td>
<td>When there is an error in submitting the translation request.</td>
</tr>
</tbody>
</table>
## Error messages in the Comparison UI

<table>
<thead>
<tr>
<th>Error message</th>
<th>Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Machine Translate</strong></td>
<td>This message appears in two scenarios:</td>
</tr>
<tr>
<td>Failed to machine translate using Microsoft. {Reason for failure}.</td>
<td>• Error message shown in the comparison UI for machine translation.</td>
</tr>
<tr>
<td><strong>Note:</strong> The reason is fetched from Dynamic Translation.</td>
<td>• Message logged in the activity stream when failed to machine translate the content.</td>
</tr>
<tr>
<td>Translations for one or more fields have failed.</td>
<td>This message appears in two scenarios:</td>
</tr>
<tr>
<td></td>
<td>• Error message shown in the comparison UI when translations for one or more fields fail.</td>
</tr>
<tr>
<td></td>
<td>• Message logged in the activity stream when translations for one or more fields fail.</td>
</tr>
<tr>
<td>Failed to machine translate.</td>
<td>Error message shown in the comparison UI in case the call for machine translate fails.</td>
</tr>
<tr>
<td><strong>Send via Email</strong></td>
<td>Message logged in the activity stream when sending source file via email fails.</td>
</tr>
<tr>
<td>Failed to send source file via email to: {email addresses}.</td>
<td>This error message appears in two scenarios:</td>
</tr>
<tr>
<td></td>
<td>• Error message persisted and shown in the comparison UI when sending the source file via email fails.</td>
</tr>
<tr>
<td></td>
<td>• Error message shown in the comparison UI in case the call for sending email fails.</td>
</tr>
<tr>
<td>Failed to send email.</td>
<td></td>
</tr>
<tr>
<td><strong>Send to TMS</strong></td>
<td>This error message appears in two scenarios:</td>
</tr>
<tr>
<td>Error while sending the task to XTM TMS for translation. {Reason for failure}.</td>
<td>• Message logged in the activity stream when sending translatable content to TMS fails.</td>
</tr>
<tr>
<td></td>
<td>• Error message persisted and shown in the comparison UI when sending translatable content to TMS fails.</td>
</tr>
<tr>
<td>Failed to send to TMS.</td>
<td>Error message shown in the comparison UI in case the call for sending translatable content to TMS fails.</td>
</tr>
<tr>
<td><strong>Retrieval from TMS</strong></td>
<td>This error appears in two scenarios:</td>
</tr>
<tr>
<td>Failed to retrieve translations from XTM TMS. {Reason for failure}.</td>
<td>• Message logged in the activity stream when retrieving translations from XTM TMS fails.</td>
</tr>
<tr>
<td></td>
<td>• Error message persisted and shown in the comparison UI when retrieving translations from XTM TMS fails.</td>
</tr>
<tr>
<td>Failed to retrieve translations from TMS.</td>
<td>Error message shown in the comparison UI in case the call for retrieving translations from XTM TMS fails.</td>
</tr>
<tr>
<td><strong>Export Source File</strong></td>
<td></td>
</tr>
<tr>
<td>Error message</td>
<td>Scenario</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Machine Translate</td>
<td></td>
</tr>
<tr>
<td>Failed to export the CSV file. [Reason for failure].</td>
<td>This error message appears in two scenarios:</td>
</tr>
<tr>
<td></td>
<td>• Error message persisted and shown in the comparison UI when exporting the source file for translations fails.</td>
</tr>
<tr>
<td></td>
<td>• Message logged in the activity stream when exporting source file for translations fails.</td>
</tr>
<tr>
<td>Failed to export file.</td>
<td>Error message shown in the comparison UI in case the call for exporting the source file for translation fails.</td>
</tr>
<tr>
<td>Import Translated File</td>
<td></td>
</tr>
<tr>
<td>Failed to import translations from CSV file. [Reason for failure].</td>
<td>This message appears in two scenarios:</td>
</tr>
<tr>
<td></td>
<td>• Message logged in the activity stream when importing the translated file fails.</td>
</tr>
<tr>
<td></td>
<td>• Error message persisted and shown in the comparison UI when importing the translated file fails.</td>
</tr>
<tr>
<td>Import failed.</td>
<td>Error message shown in the comparison UI in case the call for importing the translated file fails.</td>
</tr>
<tr>
<td>Failed to publish translations.</td>
<td>When failed to publish the translations.</td>
</tr>
<tr>
<td>Error while requesting for change.</td>
<td>When there is an error while approver requests for changes from the comparison UI.</td>
</tr>
</tbody>
</table>
Localization Insights dashboard

The Localization Insights dashboard provides the localization health of the system with reports that are generated from the localization Insights records as per the scheduled jobs. Localization Insights contain the list of artifacts with their translation statuses which, when generated, display a dashboard with information.
Required Now Platform role

- You need the localization_admin or localization_requester role to access the localization insights records for executing the scheduled jobs to generate the Localization Insights dashboard.

Use case

<table>
<thead>
<tr>
<th>User</th>
<th>Dashboard use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users with the localization_requester or localization_admin roles</td>
<td>View the localization health of the system. Request translations for Service Catalog items and Virtual Agent topics for a particular language from the Localization Insights dashboard.</td>
</tr>
</tbody>
</table>

Reports

<table>
<thead>
<tr>
<th>Title</th>
<th>Type</th>
<th>Source table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalog Items</td>
<td>Single Score</td>
<td>sn_lf_insight</td>
<td>The total number of Service Catalog items in the instance.</td>
</tr>
<tr>
<td>Languages Supported</td>
<td>Single Score</td>
<td>sys_language</td>
<td>The total number of activated languages in the instance.</td>
</tr>
<tr>
<td>Virtual Agent Topics</td>
<td>Single Score</td>
<td>sn_lf_insight</td>
<td>The total number of published Virtual Agent topics in the instance.</td>
</tr>
<tr>
<td>Translations In Progress</td>
<td>Single Score</td>
<td>sn_lf_insight</td>
<td>The total number of translations in progress in the instance.</td>
</tr>
<tr>
<td>Catalog Item Translations</td>
<td>Vertical Bar</td>
<td>sn_lf_insight</td>
<td>The total number of Service Catalog items requested for translations per language. It also indicates the following translation statuses with defined color legends:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Completely Translated</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Translation in Progress</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Partially Translated</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Not Translated</td>
</tr>
<tr>
<td>Title</td>
<td>Type</td>
<td>Source table</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>---------------</td>
<td>--------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Virtual Agent Topic Translations</td>
<td>Vertical Bar</td>
<td>sn_lf_insight</td>
<td>The total number of published Virtual Agent topics requested for translations per language. It also indicates the following translation statuses with defined color legends:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Completely Translated</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Translation in Progress</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Partially Translated</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Not Translated</td>
</tr>
<tr>
<td>Language Preferences</td>
<td>Horizontal Bar</td>
<td>localization_insights_view</td>
<td>Provides information about the number of users logged in to the instance along with their preferred languages.</td>
</tr>
</tbody>
</table>

### Request translations from Insights Dashboard

Request translations for Service Catalog items or Virtual Agent topics from the insights dashboard to localize them into the selected language based on their translation status.

Role required: localization_admin or localization_requester

1. Navigate to **Localization Framework > Insights Dashboard**.
   - The dashboard provides **Catalog Items Translations** report and **Virtual Agent Topic Translations** report by default using which you can request translations.
   - If you have created a report for your artifact to display in the dashboard, you can also request translations for the custom artifacts. For more information, see Create a report for custom artifact.

2. In the **Catalog Items Translations** report or **Virtual Agent Topic Translations** report, click the vertical bar of the language into which you want to request translations.
   - For example:
     - Select a language from the **Catalog Items Translations** report to request translations for the Service Catalog items in that language.
     - Select a language from the **Virtual Agent Topic Translations** report to request translations for the Virtual Agent topics in that language.
     - If you have a custom report created for an artifact, select a language from that report to request translations into the selected language.

3. Select one or more documents from the localization insights list.
   - You can click the **Select All** check box to request translations for all the items in the list.

4. From the **Actions on selected rows** list, select **Request Translations**.
5. Click **OK** in the Confirmation dialog box to submit the request.
Dynamic Translation

You can dynamically translate text entered in an application, such as a user-entered text on forms, for a seamless localization experience.

Get started with Dynamic Translation

1. Procure any ServiceNow, Inc. subscription that is Professional or above, and includes Dynamic Translation.
2. Activate the Dynamic Translation plugin (com.glide.dynamic_translation). For information, see Activation of Dynamic Translation.
3. Sign up and create an account with a translation service provider. By default, the following translation service providers are supported:
   - IBM. To sign up, see the IBM website.
   - Microsoft. To sign up, see the Microsoft documentation.
   - Google. To sign up, see the Google website and Set up Google Cloud Translator Service spoke.
   
   **Important:** Ensure that the Google Cloud Translator Service spoke is installed in ServiceNow Store.

4. Configure the Dynamic Translation framework for the translation service provider.

   **Note:**
   - To use the default translation service providers, you should create a connection, specify the credential information, and then activate the corresponding translator configuration.
   - Make at least one translator configuration as the default for detection to detect the language of the user-entered text.
   - Make at least one translator configuration as the default for translation to enable the Dynamic Translation experience on forms and activity streams.

You can configure your instance to use the following service providers.

   - IBM. For information about configurations for IBM, see IBM Watson Translator Service spoke.
   - Microsoft. For information about configurations for Microsoft, see Microsoft Azure Translator Service spoke.
   - Google. For information about configurations for Google, see Google Cloud Translator Service Spoke.
   - Any translation service provider of your choice. For information about configurations, see Integrate with a translation service provider.

Activation of Dynamic Translation

When you activate the Dynamic Translation plugin (com.glide.dynamic_translation), the Dynamic Translation framework is available to enable the Dynamic Translation experience on forms and activity streams. For translating the text, you can use any of the translation service providers that are available by default, or a translation service provider of your choice.

After you activate the Dynamic Translation plugin (com.glide.dynamic_translation), you can do the following tasks using a translation service provider:
• Translate user-entered text from a source language to a target language
• Detect the language of the input text

For information on activating this plugin, see Activate Dynamic Translation.

**Note:**
- If you activate the Microsoft Azure Translator Service Spoke plugin when the Dynamic Translation plugin (com.glide.dynamic_translation) is inactive, the subflows and actions of the Microsoft Azure Translator Service Spoke plugin are enabled. These subflows can be used in other flows and subflows. However, you cannot call Dynamic Translation APIs.
- If you activate the IBM Watson Translator Service Spoke plugin when the Dynamic Translation plugin is inactive, the subflows and actions of the IBM Watson Translator Service Spoke plugin are enabled. These subflows can be used in other flows and subflows. However, you cannot call Dynamic Translation APIs.

**Default Dynamic Translation framework**

By default, the Dynamic Translation plugin provides the following Dynamic Translation framework for Microsoft, IBM, and Google translation service providers.

- Connections and credential aliases and the corresponding connection attributes.

  **Note:** You should create a connection for each translation service provider and specify the credential information.

- IntegrationHub subflows and actions for these spokes.
  - IBM Watson Translator Service spoke
  - Microsoft Azure Translator Service spoke
  - Google Cloud Translator Service spoke

- Translator configurations

  **Note:** The Dynamic Translation framework is available for Google only when the Google Cloud Translator Service spoke is installed in ServiceNow Store.

**Activate Dynamic Translation**

Activate the Dynamic Translation plugin (com.glide.dynamic_translation) to enable all the required APIs.

Role required: admin

Dynamic Translation plugin (com.glide.dynamic_translation) activates these related plugins if they are not already active.

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plugin</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ServiceNow IntegrationHub Runtime</td>
<td>Enables execution of IntegrationHub actions and flows.</td>
</tr>
<tr>
<td>[com.glide.hub.integration.runtime]</td>
<td></td>
</tr>
<tr>
<td>ServiceNow IntegrationHub Action Step - REST</td>
<td>Action Step - REST</td>
</tr>
<tr>
<td>[com.glide.hub.action_step.rest]</td>
<td></td>
</tr>
<tr>
<td>Microsoft Azure Translator Service Spoke</td>
<td>Provides subflows and actions to dynamically translate the user-entered text, and to detect the language of the text using Microsoft translation services.</td>
</tr>
<tr>
<td>[com.glide.microsoft_translation_spoke]</td>
<td></td>
</tr>
<tr>
<td>IBM Watson Translator Service Spoke</td>
<td>Provides subflows and actions to dynamically translate the user-entered text, and to detect the language of the text using IBM translation services.</td>
</tr>
<tr>
<td>[com.glide.ibm_translation_spoke]</td>
<td></td>
</tr>
<tr>
<td>ServiceNow Language Detection Service Spoke</td>
<td>Uses ServiceNow® Language Detection service to provide the ability to detect the language of given text.</td>
</tr>
<tr>
<td>[com.glide.language_detection_spoke]</td>
<td></td>
</tr>
<tr>
<td>Dynamic Translation Spoke</td>
<td>Provides actions that enable the ability to translate text(s) from one language to other language(s) and to detect the language of given text.</td>
</tr>
<tr>
<td>[com.glide.dynamic_translation.spoke]</td>
<td></td>
</tr>
</tbody>
</table>

1. Navigate to **System Applications** > **All Available Applications** > **All**.
2. Find the plugin using the filter criteria and search bar. You can search for the plugin by its name or ID. If you cannot find a plugin, you might have to request it from ServiceNow personnel. For more information, see **Request a plugin**.
3. Click **Install**, and then in the Activate Plugin dialog box, click **Activate**.

**Note:** When domain separation and delegated admin are enabled in an instance, the administrative user must be in the **global** domain. Otherwise, the following error appears: Application installation is unavailable because another operation is running: Plugin Activation for <plugin name>.

DynamicTranslation API

You can use the DynamicTranslation API to translate text in real time into multiple languages using translation service providers.

This API is available as part of Server APIs, Client APIs, and Service Portal APIs to interact with translation service providers. See **DynamicTranslation - Scoped** and **DynamicTranslation - Client**.

Irrespective of the translation service provider, this API works on a standard set of inputs and outputs, and displays standard error codes and messages.

Language support limitations in the Dynamic Translation implementation

The implementation of Dynamic Translation does not support the following language translations although the corresponding I18N plugins are activated.

- Traditional Chinese. The language code at ServiceNow is different from the code used by translation service providers.
- Simplified Chinese. The language code at ServiceNow is different from the code used by translation service providers.
- Brazilian Portuguese. This language is only supported by ServiceNow and not by any other translation service providers.
- French Canada. This language is only supported by ServiceNow and not by any other translation service providers.

For information on language support, see Language internationalization support.

Language support limitations for translation service providers

Not all source language translations are supported by translation service providers. For information about language translations supported by, see the documentation. For information about language translations supported by, see the documentation for identifiable languages, and the documentation for translation models. For information about language translations supported by, see the documentation.

Microsoft Azure Translator Service spoke

Microsoft Azure Translator Service spoke provides subflows and actions to dynamically translate the user-entered texts, and to detect the language of the user-entered texts using the Microsoft translation service. Dynamic Translation supports detection and translation of single text and multiple texts.

Activate the Dynamic Translation plugin (com.glide.dynamic_translation) or the Microsoft Azure Translator Service Spoke plugin (com.glide.microsoft_translation_spoke).

Subscription

This spoke requires any ServiceNow subscription that is Professional or above, and includes Dynamic Translation.

Supported versions

API version v3

Spoke subflows

The spoke provides subflows in the Published state to integrate with Microsoft translation service. These subflows can be used as part of other subflows and flows.

<table>
<thead>
<tr>
<th>Subflow</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detect Language [detect_language_v3]</td>
<td>Contains a set of inputs, actions, and output to detect the language of the input text.</td>
</tr>
<tr>
<td>Translate Text [translate_text_v3]</td>
<td>Contains a set of inputs, actions, and outputs to translate the input text to multiple languages.</td>
</tr>
</tbody>
</table>
Note: The following subflows are deprecated in the Quebec release. These subflows are still available on instances upgraded from a previous release but not available for new instances.

- Detect Language [Deprecated] [detect_language]
- Translate Text To Multiple Languages [Deprecated] [translate_text_to_multiple_languages]

Spoke actions

The spoke provides actions to integrate with Microsoft translation services.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detect Language [detect_language_v3]</td>
<td>Detects the language of the input text.</td>
</tr>
<tr>
<td>Translate Text [translate_text_v3]</td>
<td>Translates the input text to multiple languages.</td>
</tr>
</tbody>
</table>

Note: The following actions are deprecated in the Quebec release. These actions are still available on instances upgraded from a previous release but not available for new instances.

- Detect Language [Deprecated] [detect_language]
- Translate Text To Multiple Languages [Deprecated] [translate_text_to_multiple_languages]

Microsoft account requirements

Ensure that you are registered with Microsoft and obtain the credential information. For more information, see Microsoft documentation.

For information on Microsoft Translator Text API, see the Microsoft documentation.

Connection and credential alias requirements

IntegrationHub uses aliases to manage connection and credential information. Using an alias eliminates the need to configure multiple credentials and connection information profiles when using multiple environments. If the connection or credential information changes, you do not need to update any actions that use the connection. For more information, see Credentials and connection information.

To use the spoke connection aliases, create an associated connection record and a credential record for each alias. This spoke uses the MicrosoftTranslation alias (sn_ms_trans_spoke.MicrosoftTranslation) to authorize actions.

- Connection alias requirements
  - Connection type: HTTP
  - Connection URL: For example, https://api.cognitive.microsofttranslator.com. This is a sample URL. Users can have a different URL based on their geographical preference.

Perform the following tasks to connect to the Microsoft translation services and use them to translate the dynamically generated text.
Create a credential for the MicrosoftTranslation alias

Authorize actions of Microsoft Azure Translator Service spoke by creating a credential for the MicrosoftTranslation connection and credential alias.

Role required: admin

1. Navigate to Connections & Credentials > Credentials.
2. Click New.
3. Select API Key Credentials.
4. In the API key Credentials form, fill the fields.

API key Credentials form fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Identifier of the credential.</td>
</tr>
<tr>
<td>Active</td>
<td>Option to activate the credential for use.</td>
</tr>
<tr>
<td>Applies to</td>
<td>MID servers for which the credentials are applicable. Possible options are:</td>
</tr>
<tr>
<td></td>
<td>• All MID servers in your network.</td>
</tr>
<tr>
<td></td>
<td>• Specific MID servers. In this case specify the servers in the MID servers field.</td>
</tr>
<tr>
<td>MID servers</td>
<td>Specific MID servers for which the credentials are applicable. This field is displayed only when you select Specific MID servers for the Applies to field.</td>
</tr>
<tr>
<td>Order</td>
<td>Sequence in which the credential is applied.</td>
</tr>
<tr>
<td>API Key</td>
<td>Unique code that is passed to an API to identify the connection.</td>
</tr>
<tr>
<td>Credential alias</td>
<td>Alias to use the credential.</td>
</tr>
</tbody>
</table>

5. Click Submit.

Create a connection for the MicrosoftTranslation alias

Connect to the Microsoft translation service by creating a connection. Provide information that is used by HTTP(s) actions or activities to connect to that service.

Role required: connection_admin

1. Navigate to Connections & Credentials > Connection & Credential Aliases.
2. Select the MicrosoftTranslation alias (sn_ms_trans_spoke.MicrosoftTranslation).
3. In the Connections tab, click New.
4. In the HTTP(S) Connection form, fill the fields.

HTTP(S) Connection form fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the HTTP(s) connection.</td>
</tr>
<tr>
<td>Credential</td>
<td>Credential record used to authorize the connection.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Connection alias</td>
<td>Alias record to associate with the connection. Using an alias enables you to update the connection record without having to reconfigure any actions or activities that use the alias.</td>
</tr>
<tr>
<td>Active</td>
<td>Option to activate the connection.</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain where the connection is applicable.</td>
</tr>
<tr>
<td>URL builder</td>
<td>Option to enable the system to build the connection URL. Clear this check box.</td>
</tr>
<tr>
<td>Connection URL</td>
<td>Base URL to connect to the Microsoft's translation service. For example, <a href="https://api.cognitive.microsofttranslator.com">https://api.cognitive.microsofttranslator.com</a></td>
</tr>
<tr>
<td>Use MID server</td>
<td>Option to use a MID Server for this connection. Clear this check box.</td>
</tr>
<tr>
<td>Attributes</td>
<td></td>
</tr>
<tr>
<td>Version</td>
<td>API version that the related spokes are built for. The default value is v3. Do not edit this value.</td>
</tr>
<tr>
<td>Ocp-Apim-Subscription-Region</td>
<td>Value of the regional translator resource. This value is optional when using a global translator resource. For information on supported regions, see the Microsoft documentation.</td>
</tr>
</tbody>
</table>

5. Click **Submit**.

**Activate the Microsoft translator configuration**

Make the Microsoft translation service available for use by activating the Microsoft translator configuration.

Role required: admin

1. Navigate to **Dynamic Translation > Translator Configurations**.
2. Select **Microsoft**.
3. Select the **Active** check box.
4. In the **Preferences** section, choose a translator as default either for translation or detection, or for both.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mark as default for translation</td>
<td>Option to mark the translator as default for translation.</td>
</tr>
<tr>
<td>Mark as default for detection</td>
<td>Option to mark the translator as default for detection.</td>
</tr>
</tbody>
</table>

**Note:** Make at least one translator configuration as the default configuration either for translation to enable the Dynamic Translation experience on forms and activity streams.

5. Click **Update**.
IBM Watson Translator Service spoke

IBM Watson Translator Service Spoke provides subflows and actions to dynamically translate the user-entered texts, and to detect the language of the user-entered texts using the IBM translation service. Dynamic Translation supports detection and translation of single text and multiple texts.

Activate the Dynamic Translation plugin (com.glide.dynamic_translation) or the IBM Watson Translator Service Spoke plugin (com.glide.ibm_translation_spoke).

Subscription

This spoke requires any ServiceNow subscription that is Professional or above, and includes Dynamic Translation.

Supported versions

API version v3

Spoke subflows

The spoke provides subflows in the Published state to integrate with the IBM translation services. These subflows can be used as part of other subflows and flows.

<table>
<thead>
<tr>
<th>Subflow</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detect Language [detect_language_v3]</td>
<td>Contains a set of inputs, actions, and output to detect the language of the input text.</td>
</tr>
<tr>
<td>Translate Text [translate_text_v3]</td>
<td>Contains a set of inputs, actions, and outputs to translate the input text to multiple languages.</td>
</tr>
</tbody>
</table>

Note: The following subflows are deprecated in the Quebec release. These subflows are still available on instances upgraded from a previous release but not available for new instances.

- Detect Language [Deprecated] [detect_language]
- Translate Text To Multiple Languages [Deprecated] [translate_text_to_multiple_languages]

Spoke actions

The spoke provides actions to integrate with IBM translation services.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detect Language [detect_language_v3]</td>
<td>Detects the language of the input text.</td>
</tr>
<tr>
<td>Translate Text [translate_text_v3]</td>
<td>Translates the input text to multiple languages.</td>
</tr>
</tbody>
</table>
Note: The following actions are deprecated in the Quebec release. These actions are still available on instances upgraded from a previous release but not available for new instances.

- Detect Language [Deprecated] [detect_language]
- Translate Text To Single Language [Deprecated] [translate_text_to_single_language]
- Translate Text To Multiple Languages [Deprecated] [translate_text_to_multiple_languages]

IBM account requirements

Ensure that you are registered with IBM and obtain the credential information. For more information, see IBM documentation.

For information on IBM Language Translator API, see the IBM documentation.

Connection and credential alias requirements

IntegrationHub uses aliases to manage connection and credential information. Using an alias eliminates the need to configure multiple credentials and connection information profiles when using multiple environments. If the connection or credential information changes, you do not need to update any actions that use the connection. For more information, see Credentials and connection information.

To use the spoke connection aliases, create an associated connection record and a credential record for each alias.

This spoke uses the IBMTranslation alias (sn_ibm_trans_spoke.IBMTranslation) to authorize actions.

- Connection alias requirements
  - Connection type: HTTP
  - Connection URL: Base URL provided by IBM to connect to the language translator service. Users can have a different URL based on their geographical preference.

Perform the following tasks to connect to the IBM translation services and use them to translate the dynamically generated text.

Create a credential for the IBMTranslation alias

Authorize actions of the IBM Watson Translator Service spoke by creating a credential for the IBM connection and credential alias.

Role required: admin

1. Navigate to Connections & Credentials > Credentials.
2. Click New.
3. Select Basic Auth Credentials.
4. In the Basic Auth Credentials form, fill the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Identifier of the credential.</td>
</tr>
<tr>
<td>Order</td>
<td>Sequence in which the credential is applied.</td>
</tr>
</tbody>
</table>
Create a connection for the IBMTranslation alias

Connect to the IBM translation service by creating a connection. Provide information that is used by HTTP(s) actions or activities to connect to that service.

Role required: connection_admin

1. Navigate to Connections & Credentials > Connection & Credential Aliases.
2. Select the IBMTranslation alias (sn_ibm_trans_spoke.IBMTranslation).
3. In the Connections tab, click New.
4. In the HTTP(S) Connection form, fill the fields.

HTTP(S) Connection form fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the HTTP(s) connection.</td>
</tr>
<tr>
<td>Credential</td>
<td>Credential record used to authorize the connection.</td>
</tr>
<tr>
<td>Connection alias</td>
<td>Alias record to associate with the connection. Using an alias enables you to update the connection record without having to reconfigure any actions or activities that use the alias.</td>
</tr>
<tr>
<td>Active</td>
<td>Option to activate the connection.</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain where the connection is applicable.</td>
</tr>
<tr>
<td>URL builder</td>
<td>Option to enable the system to build the connection URL. Clear this check box.</td>
</tr>
<tr>
<td>Connection URL</td>
<td>Base URL provided by IBM to connect to the language translator service. Users can have a different URL based on their geographical preference.</td>
</tr>
<tr>
<td>Use MID server</td>
<td>Option to use a MID Server for this connection. Clear this check box.</td>
</tr>
<tr>
<td>Attributes</td>
<td></td>
</tr>
<tr>
<td>Learning Opt-Out</td>
<td>Attribute to specify if your data can be used as test data by IBM to train its models. If set to true, IBM does not use your data for any API request. By default, IBM services log requests and their results.</td>
</tr>
<tr>
<td>API Version Date</td>
<td>Release date of the API version you want to use. The default value is 2018-05-01. Do not edit this value.</td>
</tr>
</tbody>
</table>

5. Click Submit.
Activate the IBM translator configuration

Make the IBM translation service available for use by activating the IBM translator configuration.

Role required: admin

1. Navigate to Dynamic Translation > Translator Configurations.
2. Select IBM.
3. Select the Active check box.
4. In the Preferences section, choose a translator as default either for translation or detection, or for both.

**Preferences**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mark as default for translation</td>
<td>Option to mark the translator as default for translation.</td>
</tr>
<tr>
<td>Mark as default for detection</td>
<td>Option to mark the translator as default for detection.</td>
</tr>
</tbody>
</table>

**Note:** Make at least one translator configuration as the default for translation to enable the Dynamic Translation experience on forms and activity streams.

5. Click Update.

**Google Cloud Translator Service spoke**

Provides subflows and actions to dynamically translate the user-entered text, and to detect the language of the text using the Google translation service.

**Request apps on the Store**

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

**Subscription**

This spoke requires one of the following subscriptions:

- Any ServiceNow subscription that is Professional or above, and includes Dynamic Translation.
- IntegrationHub Professional subscription package. For more information see, Request IntegrationHub.
**Supported versions**

Google Translate API version v3

**Scope of the spoke in the Dynamic Translation framework**

To use Google Cloud Translator Service spoke in the Dynamic Translation framework, ensure that the spoke is installed in ServiceNow Store and the Dynamic Translation plugin is active. For more information, see Dynamic Translation.

**Spoke flows**

This spoke has no sample flows.

**Spoke subflows**

The Google Cloud Translator Service spoke provides subflows in the Published state to integrate with the Google translation service. These subflows can be used as part of other subflows and flows.

<table>
<thead>
<tr>
<th>Subflow</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detect Language</td>
<td>Contains a set of inputs, actions, and outputs to detect the language of the input text.</td>
</tr>
<tr>
<td>Translate Text To Multiple Languages</td>
<td>Contains a set of inputs, actions, and outputs to translate the input text to multiple languages.</td>
</tr>
</tbody>
</table>

**Spoke actions**

The Google Cloud Translator Service spoke provides actions to integrate with the Google translation service. Available actions include:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detect Language</td>
<td>Detects the language of the input text.</td>
</tr>
<tr>
<td>Translate Text To Single Language</td>
<td>Translates the input text to a single language.</td>
</tr>
<tr>
<td>Translate Text To Multiple Languages</td>
<td>Translates the input text to multiple languages.</td>
</tr>
</tbody>
</table>

**Google account requirements**

The Google Cloud Translator Service spoke requires configuring your Google Cloud account to generate an OAuth 2.0 JWT Bearer Grant token.

**Connection and credential alias requirements**

IntegrationHub uses aliases to manage connection and credential information. Using an alias eliminates the need to configure multiple credentials and connection information profiles when using multiple environments. If the
connection or credential information changes, you don't need to update any actions that use the connection. For more information, see Connections and Credentials.

This spoke uses the GoogleTranslation alias record (sn_google_trans.GoogleTranslation) to authorize actions.

**Set up Google Cloud Translator Service spoke**

Integrate your Google account with your ServiceNow instance.

- **Role required:** admin
- Create a service account on Google Cloud, generate a service account key of JSON type and download it. For information on creating the service account key, see the Google documentation.
- Enable the Cloud Translation API service. For information on enabling a service, see the Google documentation.

**Create a Java KeyStore certificate**

Encrypt the security certificates obtained by creating a Java KeyStore (JKS) file.

- **Role required:** admin
- Download a JSON file containing the service account key from Google. For information on downloading the JSON file, see the Google documentation. Following is a sample JSON file:

```json
{
  "type": "service_account",
  "project_id": "primeval-nectar-242610",
  "private_key_id": "0c6c7b151f1c236c13005933d528bbe45314e5",
  "private_key": "-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0+3yZPcazzJi06uE7lW9XkRyEh
+qRLWzKbYzY1ZX+cmJ1NfPFpzeHrkPm\n5OQ2bjHcGCTVFCb80K1H
+VdKs7L0gTfKW2TkWfHzwO2Xv30bT+2HKBs4tTzIsMy\n+n016dGJaOk04yTIBwZc7v1r8bnGJdwh945+9NVkEPM\nG8drYJR1ImyfnnDORGR
+nypKcHAC3w7rC5E5b/V1H5KZKspR7/qxVwZS5h5PWA8b8NdrBli+YIQGGOlfjInXE
+QcE5QhiUF+Xscfgdq30cuiFo1LO9Ak/41YQb8z1Dr4r5H1UF01jp4t6fLw3k2o
+nodSr+r+XAgMBAAECggEAAAO3Q1Y9JsSwr6mEE+Ys7QGU8LW9kbsfWxMf0UtIpe
+np5e0BOEtEomodux/NKmMdJqmN80rU3G1UIitVnuW890wbVPVUsS8SVJhS7lzyv
+EvtWd1UX/x1gMFeTV34Pecag3QXy05Myq2q+pu3uYKNCrsxbN0T1XE6xU0G8i4uOL
+Yi17p7pFvctGfW50f51V1AuM8c+0rgadvOPu3JThhjauMvDFK15sbKDSdCfTqQys
+HMmNY+uhfCOr2JtGtpcC4UqggkPAUAoVRZymm1KqfnOGx0+oBDKJsd7p9D9nXvE
+nM71wq9QKSk2KsFsHNCvK4VUOBarz1qlMF1dVdxeijkQKBqQ5d7/MgN4LLeka1mE
+3r27kTka1aiq1Q1LOQRkHLbHzRexVD410oRqySszUVQXSiwZwRqLO
+hptDrNeYu\n+6WQWlwtS1Nt56r
+8Aek2mb3f+NDENFB
+RIFPdTr30G7wXeeu1+cmb8+8ESN3ehFAW\n+n7IXYTdho5c3deXNd5n9RjfrnQKggQDMqaDrRkKpwa6uq
+zSGXqFq8lXS+gppKqT\n+nUpxe45adzU5FUPUOsCEA9lBn16NDuNqi9bFBJ9T3sC
+VwBlLt2Qjz1ZPbn1lmkp\n+qNJ4T5edar826vn01WmeupAmilFqK7GoopUD
+Rito6BfSKIPczfGltu3PXLmngj\n+nRyzs5HUTwKBGc205zzscTbJnnm9YaPayNMXU7DX/
F+jhmeEco4Q1t4s5EHUTswAs69v+yhUGR7QqsG
+03u4AJQF8Ptb1CIUS5x8gBNMcLYLXHVGXuMB0WxOHzF8byRSA
+nbWhSdmCvGyPsj0x5+cOhGInYuad3R3znyT7/S1UipYh4E2/pEQEJaoGAdu1G
+MMEMNspkbD8Z5324wn77kmATPLMaFydy6LqVKSdjegj/eszKOy4e90UXFJZfJ2SEP2
+n8nrrkp4M3INq4dC16nN2Nq8yS7F5Vfmfavzca6d3IXNWqE4+Btf/40t2RRT
+HyRQk1v2R8XmgYjxXic+cWpTaik9eLDd4V79D8CgYA6Eywn9l15bVO5ksW9gyp
+0u5e1ekMNYYndPq51ywLPony9nx/y1Q3mZF17d2K7aB8p0AXKLZQv85tbgF2fvdO
+nbm4eI5Lqg8k3DZ09OohAsEuZ36JG2a1Cw4TvwqyRWe4XrdoYggk9hN84tU7u6PCsWu/
+rdB8dTSwqTFop8U=-----END PRIVATE KEY-----

"client_email": "service-now-google-trans-v3@primeval-nectar-242610.iam.gserviceaccount.com",
"client_id": "12355944370425109391",
"auth_url": "https://accounts.google.com/o/oauth2/auth",
"token_url": "https://oauth2.googleapis.com/token",
"auth_provider_x509_cert_url": "https://accounts.google.com/x509_certs",
"auth_provider_x509_cert_url": "https://accounts.google.com/x509_certs"
}
```
1. In the JSON file, perform the following for the `private_key` value.
   a) Unescape the `\n` characters.
   b) Store the private key in a file with .pem extension.

2. In the JSON file, perform the following for the `client_x509_cert_url` value.
   a) Open the link specified for `client_x509_cert_url`.
   b) Unescape the `\n` characters for the certificate associated with the `private_key_id` mentioned in the JSON file.
   c) Store the certificate value in a file with .pem extension.

3. Use the `openssl` command to create a PKCS 12 file using the recently created private key and certificate files.

   ```bash
   ```

   For example, if `certificate.pem` is the certificate and `privatekey.pem` is the private key:

   ```bash
   openssl pkcs12 -export -in certificate.pem -inkey privatekey.pem -certfile certificate.pem -out testkeystore.p12
   ```

   A PKCS 12 file, `testkeystore.p12`, is created.

4. Specify an export password or source keystore password.

   **Note:** You should specify this password when creating a JWT key for Google Cloud Translator Service spoke.

5. Use the `keytool` command to create a JKS file from the PKCS 12 file.

   ```bash
   keytool -importkeystore -srckeystore testkeystore.p12 -srcstoretype pkcs12 -destkeystore wso2carbon.jks -deststoretype JKS
   ```

   **Note:** `testKeyStore.p12` is the PKCS 12 file and `wso2carbon.jks` is the JKS file.

6. Specify a destination keystore password.

   **Note:** You should specify this password when attaching a JKS certificate to Google Cloud Translator Service spoke.

**Attach a Java KeyStore certificate to Google Cloud Translator Service spoke**

Enable the JWT client authentication by attaching a valid Java KeyStore (JKS) certificate to Google Cloud Translator Service spoke.

- Role required: admin
- Valid Java KeyStore certificate

1. Navigate to **System Definition > Certificates**.
2. Click **New**.
3. On the form, fill in the fields.

**X.509 Certificate form fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Identifier of the certificate.</td>
</tr>
<tr>
<td>Notify on expiration</td>
<td>Users to be notified when the certificate expires.</td>
</tr>
<tr>
<td>Warn in days to expire</td>
<td>Number of days to send a notification before the certificate expires.</td>
</tr>
<tr>
<td>Active</td>
<td>Option to activate the certificate.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of the certificate. Select <strong>Java Key Store</strong>.</td>
</tr>
<tr>
<td>Expires in days</td>
<td>Number of days until the certificate expires.</td>
</tr>
<tr>
<td>Key store password</td>
<td>Password to access the certificate. Use the destination keystore password specified when creating the JKS certificate. For more information on this password, see <strong>Create a Java KeyStore certificate</strong>.</td>
</tr>
<tr>
<td>Short description</td>
<td>Summary about the certificate.</td>
</tr>
</tbody>
</table>

4. Click the manage attachments icon ( ) and attach a JKS certificate.

5. To validate the JKS certificate, click **Validate Stores/Certificates**.

6. Click **Submit**.

**Create a JWT signing key for Google Cloud Translator Service spoke**

Assign a JSON Web Token (JWT) signing key to your Java KeyStore certificate.

Role required: admin

1. Navigate to **System OAuth > JWT Keys**.

2. Click **New**.

3. On the form, fill in the fields.

**JWT Keys form fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Identifier of the JWT signing key.</td>
</tr>
<tr>
<td>Signing Keystore</td>
<td>Valid JKS certificate for which you want to assign the key.</td>
</tr>
<tr>
<td>Key Id</td>
<td>Key ID to identify which key is used when multiple keys are used to sign tokens.</td>
</tr>
<tr>
<td>Signing Algorithm</td>
<td>Algorithm to sign with the key.</td>
</tr>
<tr>
<td>Signing Key Password</td>
<td>Password associated with the key. Use the export password or the source keystore password specified when creating the JKS certificate. For more information on this password, see <strong>Create a Java KeyStore certificate</strong>.</td>
</tr>
<tr>
<td>Active</td>
<td>Option to activate the key.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.
Create a JWT provider for Google Cloud Translator Service spoke

Add a JSON Web Token (JWT) provider to Google Cloud Translator Service spoke.

Role required: admin

1. Navigate to System OAuth > JWT Providers.
2. Click New.
3. On the form, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Identifier of the JWT provider.</td>
</tr>
<tr>
<td>Expiry Interval (sec)</td>
<td>Number of seconds that indicate the lifespan of the JWT provider token. Specify 3600.</td>
</tr>
<tr>
<td>Signing Configuration</td>
<td>JWT signing key.</td>
</tr>
</tbody>
</table>

4. Right-click the form header, and click Save.
5. In the Standard Claims related list, enter the values for these claims.

<table>
<thead>
<tr>
<th>Claim name</th>
<th>Claim value</th>
</tr>
</thead>
<tbody>
<tr>
<td>aud</td>
<td><a href="https://www.googleapis.com/oauth2/v4/token">https://www.googleapis.com/oauth2/v4/token</a></td>
</tr>
<tr>
<td>iss</td>
<td>client_email value from the JSON file.</td>
</tr>
</tbody>
</table>

6. In the Custom Claims related list, create the scope claim and enter its value as https://www.googleapis.com/auth/cloud-translation.
7. Click Update.

Configure the credential for the GoogleTranslation alias

Authorize actions of Google Cloud Translator Service spoke by configuring the Google OAuth 2.0 credential.

Role required: admin

1. Navigate to Connections & Credentials > Credentials.
2. Select the Google OAuth 2.0 credential.
3. Open the record specified in the OAuth Entity Profile field.
4. In the JWT Provider field, specify the JWT provider that you want to use.
5. Click Update.
6. To verify if an OAuth Access token is generated to connect to Google's translation services, click the Get OAuth Token related link of the Google OAuth 2.0 credential.

Configure the connection attributes for the GoogleTranslation alias

Connect to the Google's translation service by configuring the Google connection. Provide information that is used by HTTP(s) actions or activities to connect to that service.

Role required: connection_admin

1. Navigate to Connections & Credentials > Connections.
2. Open for the record for Google.
3. In the Attributes related list of the HTTP(S) Connection form, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value required</th>
</tr>
</thead>
<tbody>
<tr>
<td>location</td>
<td>Location of the customer. If the value is not specified when creating an account on Google Cloud, then specify <code>global</code>.</td>
</tr>
<tr>
<td>project_id</td>
<td>Identifier of a project. Specify the <code>project_id</code> value from the JSON file.</td>
</tr>
<tr>
<td>version</td>
<td>API version that the related spokes are built for. The default value is <code>v3beta1</code>. Because Google now supports the v3 version, you can override this value as <code>v3</code>.</td>
</tr>
</tbody>
</table>

4. Right-click the form header and click **Save**.

**Dynamic Translation spoke**

The Dynamic Translation spoke provides actions to enable the ability to translate multiple texts from one language into one or more languages and detect the language of multiple texts seamlessly.

The Dynamic Translation APIs are accessible across the ServiceNow platform through the following access points:

- Server
- Platform Client
- Portal Client

In the Quebec release, the Dynamic Translation spoke enables you to access the Dynamic Translation APIs from the Flow Designer.

The Dynamic Translation Spoke is a plugin (com.glide.dynamic_translation.spoke) that is available with activation of the Dynamic Translation plugin (com.glide.dynamic_translation).

The Dynamic Translation spoke contains actions that are built corresponding to the Dynamic Translation APIs. The following actions are built in the Quebec release in Dynamic Translation spoke:

<table>
<thead>
<tr>
<th>Action Name</th>
<th>API</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detect Language</td>
<td><code>getDetectedLanguage()</code></td>
</tr>
<tr>
<td>Detect Languages</td>
<td><code>getDetectedLanguages()</code></td>
</tr>
<tr>
<td>Translate Text</td>
<td><code>getTranslation()</code></td>
</tr>
<tr>
<td>Translate Texts</td>
<td><code>getTranslations()</code></td>
</tr>
<tr>
<td>Is Dynamic Translation Enabled</td>
<td><code>isDynamicTranslationEnabled()</code></td>
</tr>
</tbody>
</table>

For more information about accessing the actions from the Flow Designer, see **Access Dynamic Translation spoke actions from the Flow Designer**.
Access Dynamic Translation spoke actions from the Flow Designer

Access Dynamic Translation spoke actions from the Flow Designer to dynamically detect and translate the given texts.

- Ensure that the Dynamic Translation spoke is activated with Dynamic Translation plugin (com.glide.dynamic_translation) activation and configure the Dynamic Translation framework for a translation service provider.
- Role required: admin

2. Click the Actions tab.
3. Search the actions using the filter criteria and search bar.
   You can search for the actions with the spoke’s name. For example, Dynamic Translation.
   All the actions built in the Dynamic Translation spoke are displayed.
   For more information, see Actions in Dynamic Translation spoke.

Actions in Dynamic Translation spoke

Actions in Dynamic Translation spoke are built to access the Dynamic Translation APIs from the Flow Designer.

<table>
<thead>
<tr>
<th>Dynamic Translation Spoke actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
</tr>
<tr>
<td>Detect Language [detect_language]</td>
</tr>
<tr>
<td>Detect Languages [detect_languages]</td>
</tr>
<tr>
<td>Is Dynamic Translation Enabled</td>
</tr>
<tr>
<td>Translate Text [translate_text]</td>
</tr>
<tr>
<td>Translate Texts [translate_texts]</td>
</tr>
</tbody>
</table>

Standard Error Codes

When an error occurs, error codes populate with the reason for the error. Refer to the following information for the standard error codes that appear while you work on the Dynamic Translation spoke actions corresponding to the Dynamic Translation APIs:

- Dynamic Translation- Scoped
Language Detection spoke

ServiceNow Language Detection Service spoke provides a single subflow and action to detect the language of the given text using the ServiceNow language detection service.

The ServiceNow Language Detection Service spoke is an in-house language detection service offered by ServiceNow platform in the Quebec release.

The ServiceNow Language Detection Service spoke plugin (com.glide.language_detection_spoke) is available with the activation of Dynamic Translation plugin (com.glide.dynamic_translation).

Subscription

This spoke requires any ServiceNow subscription that is Professional or above, and includes Dynamic Translation.

Supported versions

API version v3

Spoke subflow

The spoke provides the subflow in the Published state to integrate with the ServiceNow language detection service.

Spoke action

The spoke provides the action in the Published state to integrate with the ServiceNow language detection service.

The ServiceNow Language Detection service uses the following Dynamic Translation APIs to detect the language of the input texts:

- getDetectedLanguage: Provides text to identify the languages.
Integrate with a translation service provider

Integrate with any translation service provider of your choice to translate the dynamically generated text.

Role required: admin

1. Create subflows to detect the language of the input text, and translate the input text. Use IntegrationHub subflows, actions, and connections and credentials. See Flow Designer.
   a) Ensure that the mapping for error messages is done to map error codes from the translation service provider to the error codes and standardized error messages supported by ServiceNow.

<table>
<thead>
<tr>
<th>Error code</th>
<th>Error message</th>
</tr>
</thead>
<tbody>
<tr>
<td>40050</td>
<td>Error code to populate error messages from the translator service provider instead of standardized error messages.</td>
</tr>
<tr>
<td>40051</td>
<td>Unknown error occurred.</td>
</tr>
<tr>
<td>40052</td>
<td>Text ('text' field) has exceeded its maximum length.</td>
</tr>
<tr>
<td>40053</td>
<td>Source language is invalid.</td>
</tr>
<tr>
<td>40054</td>
<td>Target language is invalid.</td>
</tr>
<tr>
<td>40055</td>
<td>Request is not authorized because credentials are missing or invalid.</td>
</tr>
<tr>
<td>40056</td>
<td>Text cannot be translated to target languages.</td>
</tr>
</tbody>
</table>

b) Ensure that the inputs and output fields are in the following format for subflows.

**Note:** While you create subflows, you can refer to the subflows that are available by default if required. For example, Detect Language [detect_language_v3] and Translate Text To Multiple Languages [translate_text_to_multiple_languages_v3].
### Field name | Description | Type
---|---|---
detections | Information about the code and confidence of the languages detected by the translator and their respective alternatives, error codes, and error messages. | Array.Object. Each element of the Object is a String value.
  - **Code**: Language code of the detected language as specified by the translation service provider.
  - **Confidence**: Value that indicates the confidence in the result. The value is between zero and one. A low value indicates a low confidence.

For example, French text with confidence of 0.93

```json
{ 'code' : 'fr',
  'confidence' : '0.93' }
```

For more information refer to the `getDetectedLanguages` section of DynamicTranslation - Scoped.

status | Status of the request. | Choice

---

### Translate subflow

#### Field name | Description | Type
---|---|---
Inputs | | 
texts | Texts to be translated. In the Quebec release, version v3 supports bulk translation-translation of multiple texts input in a single string. | Array.String

target_languages | Array of language codes to which the text needs to be translated. For example, | Array.String. Each element of the array is a String value.

```python
['fr', 'it']
```

source_language | Language code of the source text. For example, | String

```python
'en'
```
### Field name | Description | Type
---|---|---
additional_parameters | Array of additional parameters. For example, 

```
[{'parameter_name': 'textType',
  'parameter_value': 'html'}]
```
| Array.Object. Each element of the array is an Object with String values. |

**Outputs**

<table>
<thead>
<tr>
<th>Field name</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
</table>
| translations | Translated texts in the specified target languages. Each element of the array is an Object containing target language and the translated text. For example, 

```
[
  {'target_language': 'fr',
   'translated_text': 'Bonjour'},
  {'target_language': 'it',
   'translated_text': 'ciao'}
]
```
| Array.Object. Each element of the array is an Object with String values. |

**Note:** For more information refer to the `getTranslations` section of `DynamicTranslation - Scoped`.

<table>
<thead>
<tr>
<th>Field name</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>status</td>
<td>Status of the request.</td>
<td>Choice</td>
</tr>
</tbody>
</table>

---

**Note:** Ensure that the Run As field is set to User who initiates session in the flow properties.

2. Create a translator configuration and activate it. See [Create a translator configuration](#).

**Create a translator configuration**

Configure the Dynamic Translation framework for a translation service provider of your choice to dynamically translate the user-entered text in the application.

**Role required:** admin

Ensure that the Dynamic Translation plugin (com.glide.dynamic_translation) is activated.

1. Navigate to Dynamic Translation > Translator Configurations.

   **Note:** By default, ServiceNow, Google, IBM, and Microsoft translator configurations are available.

2. Click New.
3. In the Translator Configuration form, fill the fields.

**Translator Configuration form fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Identifier of the translator configuration.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Active | Activates the translator configuration.
Version | Version of the contract used in subflows. The default value is v3 that uses complex objects in the input and output fields of subflows.

**Note:** Versions v1 and v2 accept only a single string and are deprecated. It is recommended to use version v3 that accepts multiple strings for translation and detection.

Preferences

Choose a translate subflow | IntegrationHub subflow that interacts with the translation service provider to translate the input text.

Mark as default for translation | Specifies the translator configuration as the default configuration for translation.

When no translator configuration is specified while translating the text, then the default configuration is used.

**Note:**
- The configuration should be active to make it default.
- You can select only one configuration as default for translation.

Choose a detect subflow | IntegrationHub subflow that interacts with the translation service provider to detect the language of the input text.

Mark as default for detection | Specifies the translator configuration as the default configuration for detection.

When no translator configuration is specified while detecting the text, then the default configuration is used.

**Note:**
- The configuration should be active to make it default.
- You can select only one configuration as default for translation.

### 4. Click Submit.

**Migrate to version v3 of a translator configuration**

Implement the contract with subflows using complex objects in the input and output fields for dynamic translation of text.

Role required: admin
For a translator configuration that you added to integrate with a translation service provider of your choice, implement IntegrationHub subflows with complex objects in the input and output fields. These subflows are required to interact with the translation service provider for the following tasks:

- Translate the input text
- Detect the language of the input text

For information on implementing these subflows, see Integrate with a translation service provider.

After an upgrade to Quebec, the version of all translator configurations that are available by default but not customized is automatically updated to v3. The corresponding subflows have complex objects in the input and output fields.

However, you should migrate to version v3 for the following translator configurations:

- Translator configurations that are available by default but customized in New York
- Translator configuration that you added to integrate with a translation service provider of your choice

1. Navigate to Dynamic Translation > Translator Configurations.
2. Select a translator configuration.
3. In the Translator Configuration form, update these fields.

**Translator Configuration form fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Activates the translator configuration to integrate with Dynamic Translation.</td>
</tr>
<tr>
<td>Version</td>
<td>Version of the contract used in subflows. Select v3.</td>
</tr>
<tr>
<td>Choose a translate subflow</td>
<td>IntegrationHub subflow with complex objects in the input and output fields to translate the input text.</td>
</tr>
<tr>
<td></td>
<td>• For the translator configurations that are available by default but customized, select Translate Text [translate_text_v3].</td>
</tr>
<tr>
<td></td>
<td>• For the translator configuration that you added to integrate with a translation service provider of your choice, select the subflow that you implemented with complex objects. The contract now supports multiple texts in a single method call.</td>
</tr>
<tr>
<td>Choose a detect subflow</td>
<td>IntegrationHub subflow with complex objects in the input and output fields to detect the language of the input text.</td>
</tr>
<tr>
<td></td>
<td>• For the translator configurations that are available by default but customized, select Detect Language [detect_language_v3].</td>
</tr>
<tr>
<td></td>
<td>• For the translator configuration that you added to integrate with a translation service provider of your choice, select the subflow that you implemented with complex objects. The contract now supports multiple texts in a single method call.</td>
</tr>
<tr>
<td>Mark as default for translation</td>
<td>Marks the translator as the default configuration for dynamic translation of text.</td>
</tr>
</tbody>
</table>
4. Click **Update**.

**Limitations in Dynamic Translation**

You need to be aware of a few limitations when you integrate with a translation service provider to enable the Dynamic Translation experience.

**Length limitations for translation service providers**

Following are the length limitations for translation service providers:

- For Microsoft, the input text for translation cannot have more than 10000 characters including spaces. And the limit for the input text for detection is 50000. For more information, see [Microsoft Documentation](#).
- For IBM, the size of the input text cannot exceed 50KB. For more information, see [IBM Documentation](#).
- For Google, the recommended maximum length of each request is 5k characters. The maximum size of the input text cannot exceed 30K code points. For more information, see [Google Documentation](#).

**Language support limitations in the Dynamic Translation implementation**

The implementation of Dynamic Translation does not support the following language translations although the corresponding I18N plugins are activated.

- Traditional Chinese. The language code at ServiceNow is different from the code used by translation service providers.
- Simplified Chinese. The language code at ServiceNow is different from the code used by translation service providers.
- Brazilian Portuguese. This language is only supported by ServiceNow and not by any other translation service providers.
- French Canada. This language is only supported by ServiceNow and not by any other translation service providers.

For information on language support, see [Language internationalization support](#).

**Language support limitations for translation service providers**

Not all source language translations are supported by translation service providers.

For information about language translations supported by Microsoft, see the [documentation](#).

For information about language translations supported by IBM, see the [documentation](#) for identifiable languages, and the [documentation](#) for translation models.

For information about language translations supported by Google, see the [documentation](#).
Dynamic translation on forms and activity streams

For a seamless localization experience on forms and activity streams, you can dynamically translate text based on the preferred language of a user.

Dynamic translation on forms

You can translate the field values on forms in Platform.

To enable dynamic translation at the field-level on Platform forms, see Enable dynamic translation for a field. Once enabled, click to show or hide the translated content.

Dynamic translation in activity streams

You can translate activity streams both in Platform and Service Portal.

Dynamic translation is enabled by default for comments and work notes in the activity stream. Click translate to show or hide the translated content for each comment or work note.

Note: You cannot translate activity streams in Agent Workspace.

Length limitations for translation service providers

Following are the length limitations for translation service providers:

- For , the input text for translation cannot have more than 10000 characters including spaces. And the limit for the input text for detection is 50000. For more information, see Microsoft Documentation.
- For , the size of the input text cannot exceed 50KB. For more information, see IBM Documentation.
- For , the recommended maximum length of each request is 5k characters. The maximum size of the input text cannot exceed 30K code points. For more information, see Google Documentation.

Enable dynamic translation for a field

Translate the dynamically generated text for a field on Platform forms by enabling the field-level dynamic translation.

You can translate the text based on the preferred language of a user.

Role required: admin

Activate the Dynamic Translation plugin (com.glide.dynamic_translation).

Dynamic Translation supports only the following field types:

- String
- String (Full UTF-8)
- Multi Line Small Text Area
- Wide Text

Note:
• Following are the length limitations for translation service providers:
  • For , the input text for translation cannot have more than 10000 characters including spaces. And the limit for the input text for detection is 50000. For more information, see Microsoft Documentation.
  • For , the size of the input text cannot exceed 50KB. For more information, see IBM Documentation.
  • For , the recommended maximum length of each request is 5k characters. The maximum size of the input text cannot exceed 30K code points. For more information, see Google Documentation.
  • You cannot translate a field on Agent Workspace forms.

 1. Navigate to any form. For example, an Incident form.
  2. Right-click the required field and select Configure Dictionary.
  3. In the Attributes related list, click New.
  4. In the Dictionary Attribute form, fill the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute</td>
<td>Dynamic Translation Enabled</td>
</tr>
<tr>
<td>Value</td>
<td>true</td>
</tr>
</tbody>
</table>

 5. Click Submit.
  6. Click Update.

A translate icon appears next to the field. The logged-in user can click this icon to translate the text to the user’s preferred language using the default translation service provider specified in the translator configurations. For information about error messages during translation, see Error messages for dynamic translation on forms and activity streams.

Note: If you do not have any default translator configuration, you cannot view the translate icon.
Error messages for dynamic translation on forms and activity streams

Error messages are displayed when the text cannot be dynamically translated on forms activity streams.

### Error messages

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Error message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field has no value.</td>
<td>No text to translate.</td>
</tr>
<tr>
<td><strong>Note:</strong> This scenario is applicable only for fields on the form.</td>
<td></td>
</tr>
<tr>
<td>Text to be translated is already in the logged-in user's preferred language.</td>
<td>This content is written in your preferred language. No need to translate.</td>
</tr>
<tr>
<td>Text cannot be translated to the user's preferred language by the default translation service provider.</td>
<td>Text cannot be translated to your preferred language.</td>
</tr>
<tr>
<td>Credentials configured for the translation service provider under Connections &amp; Credentials are not valid.</td>
<td>Credentials are missing or invalid. Contact your administrator.</td>
</tr>
<tr>
<td>Text to be translated has exceeded the maximum length supported by the default translation service provider.</td>
<td>Text has exceeded the maximum length.</td>
</tr>
<tr>
<td>Error during translation. Possible reasons are:</td>
<td>Unable to translate.</td>
</tr>
<tr>
<td>• Credentials configured for the translation service provider under the Connections &amp; Credentials sub module are missing.</td>
<td></td>
</tr>
<tr>
<td>• Translation got timed out.</td>
<td></td>
</tr>
<tr>
<td>• Any other issue with the translation service provider. For example, the exhaustion of credentials for more transactions.</td>
<td></td>
</tr>
</tbody>
</table>

### Translate a knowledge article

You can start translating articles once they are published and assigned to you for translation.

Role required: admin, knowledge_admin, or knowledge

1. Navigate to Knowledge > Translation Management > My Assigned Tasks.
2. In the Knowledge Translation Tasks page, select one of the listed translation tasks assigned to you. The Knowledge Translation Tasks page lists all knowledge translation tasks assigned to you.
3. Click **Translate**.

**Note:** If you want to do a translation directly from an article, use the **Translate** related link on the article page.

The **Translate from** and **Translate to** panes are side-by-side for easy viewing, as shown in the following figure.

4. Click **Machine translate**, which automatically translates to the targeted languages.

**Note:** A default translator configuration should be available. For configuring the translation API, see **Dynamic Translation**.

5. Click **Create draft article** to create a draft version of the translated article.

If a translated article is already present for that language, a new draft version overwrites an existing translated content.

6. Click **Publish**.

The newly created draft is listed in the **Translated Versions** tab.
Dynamic Translation for Agent Chat Overview

Dynamic Translation for Agent Chat (DTAC) translates chat messages from one language to another. DTAC enables agents and end users to have a chat conversation with each other, without the need of a shared language.

DTAC translates the chat text for the agent and the end user. For example, if the end user enters German text, the agent automatically receives that text translated into the agent’s preferred language, for example, English. Likewise, when the agent responds with English text, it appears to the end user in German. When DTAC is enabled, the end user only sees text translated into the end user’s language. The agent’s and end user’s preferred languages are specified in the instance configuration.

DTAC is disabled by default and can be enabled by the system administrator. If an agent turns off DTAC in their chat window session, DTAC stops translating the chat text for the agent and end user from that point on. DTAC will not translate the previous text. If the agent turns DTAC back on during the session, it translates the chat text from that point on for the agent and end user.

DTAC supports various translation services including Google Cloud Translator Service, IBM Translator Service, and Microsoft Azure Translator Service. DTAC can translate in the languages supported by these translation services. Even though the corresponding I18N plugins are activated, DTAC does not support the following language translations:

- simplified and traditional Chinese
- Brazilian Portuguese
- Canadian French

DTAC is also available for Agent Chat in mobile for iOS and Android.

Before installing the DTAC plugins, you must complete the Dynamic Translation setup steps. For more information, see Activate Dynamic Translation.

For an overview about how Agent Chat works, see Workspace Agent Chat.

For information about Dynamic Translation, see Dynamic Translation.

Domain separation and Dynamic Translation

Domain separation is supported in Dynamic Translation and is configured to apply to translator configurations. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can control several aspects of this separation, including which users can see and access data.

Support level: Basic

- Business logic: Ensure that data goes into the proper domain for the application’s service provider use cases.
- The application supports domain separation at run time. The domain separation includes separation from the user interface, cache keys, reporting, rollups, and aggregations.
- The owner of the instance must set up the application to function across multiple tenants.

Use case: When a service provider (SP) uses chat to respond to a tenant-customer’s message, the client must be able to see the SP's response.

To learn more, see Application support for domain separation.
**Activation information**

You should activate the Domain Support - Domain Extensions Installer plugin (com.glide.domain.msp_extensions.installer). For information on how you can request for the plugin activation, see Request for domain separation in Dynamic Translation.

**How domain separation works in Dynamic Translation**

A service provider with domain separated instances can implement the Dynamic Translation framework so that users can use the translation service providers configured in the translator configurations specific to their domain. Translator configurations are process-separated in Dynamic Translation. All translation service providers configured in the translator configurations of the parent domain are available in child domains.

A translator configuration in the global domain is visible in all other domains. In any domain, a user can only view the translator configurations configured in the following domains:

- Current domain
- Parent domains
- Global domain

**Note:** If there are multiple translator configurations in a domain for the same translation service provider, the translator configuration of the current domain or the closest parent domain is considered for dynamic translation.

Also, different connections can be configured for the same connection and credential alias of a translation service provider in multiple domains. However, Credentials and Connections are data-separated. So, a connection configured in a child domain is visible in parent domains. For information on domain separation for Connections and Credentials, see Domain separation for Credentials and Connections.

For example, consider the following scenario:
Different connections are configured for the same connection and credential alias of Google in multiple domains. When in Domain A, all the following connections are visible:

- Connection1
- Connection2
- Connection3

**Note:** When multiple active connections are visible for the same connection and credential alias in a domain, the connection with the highest order is given priority when the Support Multiple Active Connections check box is selected.

**Domain-separated table**

Translator Configuration [sn_dt_translator_configuration]

**Default translator configuration for a domain**

The default translator configuration of the current domain is always considered for dynamic translation. If the current domain does not have any default translator configuration, then the available default translator configuration of the nearest parent is considered.

A domain can have multiple default translator configurations. In this case also, the default translator configuration of the current domain is considered for dynamic translation. For example, let us consider the following scenario:

![Diagram of domains A, B, and C with TC1, TC2, and TC3]

**Domain separation in Dynamic Translation**

In Domain B, both TC1 and TC2 are visible. From Domain B, TC2 is first set as the default translator configuration. From Domain A, TC1 is then overridden and set as the default translator configuration. This results in multiple default translator configurations in Domain B. In this case, when in Domain B, TC2 is used as the default translator configuration for dynamic translation.
Overriding a translator configuration

In any domain, you can override the translator configuration of that domain or the parent domain. The overridden translator configuration of a parent domain is also visible in child domains. However, the overridden translator configuration of a child domain is not visible in the parent domain.

After you override a translator configuration of the same domain, only the overridden translator configuration is visible in that domain.

After you override a translator configuration of a parent domain, the following scenarios happen:

• Only the overridden translator configuration is visible in the child domain.
• The **Overrides** field of overridden translator configuration refers to the original translator configuration of the parent domain.

For example, consider the following scenario:

![Diagram of domain separation in Dynamic Translation](image)

**Domain separation in Dynamic Translation**

You can override a translator configuration TC1 from Domain B. After overriding, only the overridden configuration TC1 is available in Domain B and the **Overrides** field of TC1 refers to **TC1** of the parent domain.

**Request for domain separation in Dynamic Translation**

Enable the support for the Dynamic Translation framework in domain-separated instances.

Role required: admin

There are two ways to request a plugin:

• Access the Now Support Service Catalog directly by clicking **Service Catalog > Activate Plugin** on Now Support.
• Access the Now Support Service Catalog through the All Applications page on your instance by following these steps.

1. Navigate to **System Applications > All Available Applications > All.**
2. On the All Applications page, click **Request Plugin** to open the Request form on HI.
3. On Now Support, select the redirect link to access the Now Support Service Portal Service Catalog.

<table>
<thead>
<tr>
<th>Activate Plugin</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>In order to enhance the user experience, we have redesigned Activate a Plugin service catalog. Please use the new Hi Service Portal 'Activate a Plugin' service catalog item. You can also use Manage Instances page on Service Portal to Activate a Plugin.</td>
<td></td>
</tr>
<tr>
<td>Take me to the Hi Service Portal Activate a Plugin Service Catalog.</td>
<td></td>
</tr>
</tbody>
</table>

4. On the form, fill in the fields.

### Activate Plugin request form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Instance</td>
<td>Instance on which to activate the plugin.</td>
</tr>
<tr>
<td>Plugin Name</td>
<td>Name of the plugin to activate.</td>
</tr>
<tr>
<td>Specify the date and time you would like this plugin to be enabled</td>
<td>The date and time must be at least two business days from the current time.</td>
</tr>
</tbody>
</table>

**Note:** Plugins are activated in two batches, once in the morning and once in the evening, on every business day in the US Pacific time zone. If the plugin must be activated at a specific time, enter the request in the Reason/Comments field.

| Reason/Comments | Information that would be helpful for the ServiceNow personnel who are activating the plugin. For example, if you need the plugin activated at a specific time instead of during one of the default activation windows, specify that in the comments. |

5. Click **Submit**.

### Time configuration

Time configuration includes the scheduling of events and tracking of time. There are several functions available that enable tracking of time and using that information across applications.

### Date and time fields

Time can be stored in different ways in records. Understanding how time is stored underlies efficient use of time functions. To learn more, see Use Date and Time Fields.
Time zones

The Now Platform stores time values in Universal Coordinated Time. Times appear globally based on the system time zone, but appear to users in their local time zone, based on their own user settings. To avoid calculation errors or confusing outputs, proper use of time zone information is critical.

- All dates and times gathered through web services appear in GMT.
- When you insert data using a web service, it uses the time zone defined for the active user.
- If the active user does not have a specified time zone, it instead uses the system time zone.

Business calendars and schedules

You create business calendars in the Now Platform so that you can schedule events for your users and track their time across applications. You can define several types of schedules and calendars, including fiscal calendars, in the Business Calendar menu. To learn more about business calendars, see Creating business calendars.

The legacy schedules functions consist of rules that include or exclude ranges of time for certain time-related functionality. For example, schedules can restrict SLAs to only count time during business hours. To learn more about legacy schedule definition, see Creating and using schedules.

Time display

There are several useful user interfaces that help represent time visually. To learn more, see Displaying Time.

Viewing logs

Logs within the system provide historical information as to what occurred in the instance when.

Scheduling events

Scheduling events enable other functionality to be triggered at particular times, or in response to specific events. To learn more, see Schedule Events.

Timing functionality

These functions gather information with regards to duration. They answer the question "How long?", and if time events can be based on that information. To learn more, see Timing Functionality.

Date and Date/Time fields

Records in the Now Platform store date and time values in several different types of fields. These values are stored as integer numbers, in milliseconds, and appear in the appropriate date or date/time format.

Date and Date/Time field types

The Now Platform stores date and date/time information in records using the following field types:
### Date and time field types

<table>
<thead>
<tr>
<th>Field type</th>
<th>Dictionary XML type</th>
<th>MySQL DB type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>glide_date</td>
<td>DATE</td>
</tr>
<tr>
<td>Date/Time</td>
<td>glide_date_time</td>
<td>DATETIME</td>
</tr>
<tr>
<td>Time</td>
<td>glide_time</td>
<td>DATETIME</td>
</tr>
<tr>
<td>Duration</td>
<td>glide_duration</td>
<td>DATETIME</td>
</tr>
<tr>
<td>Due date</td>
<td>due_date</td>
<td>DATETIME</td>
</tr>
</tbody>
</table>

For the full listing of field types, see Introduction to Fields.

### Global date and time field format

You define default date and time formats globally using system properties.

#### Date format

The `glide.sys.date_format` property defines the date format. An administrator can modify the property by navigating to **System Properties > System**. The default format is: yyyy-MM-dd.

**Note:** A user can override the global date or time format with a personal preference.

Modifying the `glide.sys.date_format` property changes the date or time format globally. When modifying the standard date format, also verify the format using a **Validate Date and Time** script. You can use the same pattern strings as the `java.text.SimpleDateFormat` class, with the following exception:

- You cannot append the 'z' character to include the time zone when adding it to a script.
- If the resulting time zone is not three characters, an **Invalid Date appears** error appears when you validate the script, because the Date/Time Validation Script (`sys_script_validator`) fails. This failure occurs even though the script debugger shows that the content of the value meets the requirement of 'g_user_date_time_format'.

**MM** is months, while **mm** indicates minutes. The format string consists of the following abbreviations.

<table>
<thead>
<tr>
<th>Field</th>
<th>Full form</th>
<th>Short form</th>
</tr>
</thead>
<tbody>
<tr>
<td>Year</td>
<td>yyyy (4 digits)</td>
<td>yy (2 digits), y (2 or 4 digits)</td>
</tr>
<tr>
<td>Month</td>
<td>MMM (name or abbr.)</td>
<td>MM (2 digits), M (1 or 2 digits)</td>
</tr>
<tr>
<td>Day of Month</td>
<td>dd (2 digits)</td>
<td>d (1 or 2 digits)</td>
</tr>
</tbody>
</table>

**Note:** It is recommended that you use a yyyy format-based date. For example, use mm-dd-yyyy, yyyy-mm-dd, or dd-mm-yyyy.

- If your system date format is set to use the yy year format, the system considers dates 20 years later or 80 years earlier from the current date as a date in the past or future leading to an unexpected behavior.
- For example, if you set the year as 51 for 2051, the system considers the year as 1951. Similarly, if you set the year as 37 for 1937, the system considers the year as 2037.
Time format

An administrator can modify the property by navigating to **System Properties > System**. Modifying the property changes the date or time format globally. When modifying the standard time format, also verify the format using a Validate Date and Time script. You can use the same pattern strings as the java.text.SimpleDateFormat class, with minor exceptions. The format string consists of the following abbreviations.

<table>
<thead>
<tr>
<th>Field</th>
<th>Full form</th>
<th>Short form</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hour (1-12)</td>
<td>hh (2 digits)</td>
<td>h (1 or 2 digits)</td>
</tr>
<tr>
<td>Hour (0-23)</td>
<td>HH (2 digits)</td>
<td>H (1 or 2 digits)</td>
</tr>
<tr>
<td>Minute</td>
<td>mm (2 digits)</td>
<td>m (1 or 2 digits)</td>
</tr>
<tr>
<td>Second</td>
<td>ss (2 digits)</td>
<td>s (1 or 2 digits)</td>
</tr>
</tbody>
</table>

Add the character a to the end of the time format string to indicate AM or PM. This option shows AM or PM whether you are using 12-hour time (hh) or 24-hour time (HH).

The default format is: HH:mm:ss.

**Note:** A user can override the global date or time format with a personal preference.

Personalize the system date format

You can personalize the format in which date values appear in your instance.

Personalizing the date format does not change global settings or impact the way other users see date values.

**Note:** It is recommended that you use a yyyy format-based date. For example, use mm-dd-yyyy, yyyy-mm-dd, or dd-mm-yyyy.

- If your system date format is set to use the yy year format, the system considers dates 20 years later or 80 years earlier from the current date as a date in the past or future leading to an unexpected behavior.
- For example, if you set the year as 51 for 2051, the system considers the year as 1951. Similarly, if you set the year as 37 for 1937, the system considers the year as 2037.

1. Navigate to **Self-Service > My Profile**.
2. In the **Date format** field, select an option.
3. Click **Update**.

Personalize the system time format

You can personalize the format in which time values appear in your instance.

An administrator must add the **Time format** field to the Self-Service view of the User form. For more information, see **Configuring the form layout**.

Personalizing the time format does not change global settings or impact the way other users see time values.

1. Navigate to **Self-Service > My Profile**.
2. In the **Time format** field, select an option.
3. Click **Update**.
Configure the date picker for the list editor

A system property enables you to choose between two date picker configurations for the list editor.

Role required: admin

1. Navigate to `sys_properties.list`.
2. Search for the property named `glide.ui.list_edit.show_calendar_only`.
3. Set the property **Value** to either of the following options.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>false</td>
<td>Calendar as well as a field appears for a date picker for manual date entry.</td>
</tr>
<tr>
<td>true</td>
<td>Calendar only appears for a date picker, which is the default behavior in UI16 and UI15.</td>
</tr>
<tr>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Default date and time fields</strong></td>
<td>Certain time fields are provided by default to store particular date and time fields.</td>
</tr>
<tr>
<td><strong>Global timestamp fields</strong></td>
<td>All records inherit certain time stamp fields from the Global [global] table.</td>
</tr>
<tr>
<td>• Created</td>
<td></td>
</tr>
<tr>
<td>• Updated</td>
<td></td>
</tr>
<tr>
<td>These fields are automatically populated with the correct date and time, expressed in Greenwich Mean Time (GMT), rather than in the logged in user's local time zone.</td>
<td></td>
</tr>
<tr>
<td><strong>Planned Task time fields</strong></td>
<td>The Planned Task plugin provides a table (Planned Task [planned task]) with standard fields for measuring a planned task's time. For more information, see Planned Task.</td>
</tr>
<tr>
<td><strong>Task fields for measuring work time</strong></td>
<td>Use default task fields to measure progress and resolution for certain records.</td>
</tr>
<tr>
<td>The following base system fields are provided on certain tables to track how long it takes to close tickets:</td>
<td></td>
</tr>
<tr>
<td>• Time worked: A timer that runs when you view the record, and pauses while you close it, or when you manually pause it. Used to track the time spent by the help desk while working on the record.</td>
<td></td>
</tr>
<tr>
<td>• Resolve time: A calculated field that measures the time from the moment the record is opened, to the moment the record is closed. Used to track how long it takes to resolve the record.</td>
<td></td>
</tr>
</tbody>
</table>
These fields provide different metrics for request response.

The following additional tools are available for tracking work time:

- **Service level agreements (SLAs)**: Measures how long it takes a record to fulfill certain conditions (such as an incident being marked Resolved).
- **Time cards**: Use the Time worked field to break down how much time was spent by day of the week.

**Time worked**

The Task [task] table provides a time-tracking field called Time worked.

![Time worked field](image)

This field measures how long a record has been viewed to track work time on a ticket. Any table that extends Task can use this field. To add the field, configure the form.

As the record is viewed, the timer counts upward. To pause the timer, click the stop icon ( ).

To resume the timer, click the start icon ( ).

When you save a task, the amount of new time in the timer is used to generate a record on the Time Worked [task_time_worked] table. You can view this table as a related list on the task form.

By default, the time in the Time worked field is a cumulative value stored in the task record. If you modify a Time Worked record, the changes are not reflected in the task timer.

You can set the property `com.snc.time_worked.update_task_timer` to enable updating of the task timer value, based on changes to the Time worked records. You do this using the Update task timer business rule.

**Resolve time**

The Resolve time field is available on the Incident [incident] and Request [sc_request] tables. This field allows for easy reporting on how long it takes for requests to be closed, and is stored as an integer number of seconds.

### Business rule calculation

Specific business rules calculate the Resolve time field when the record is resolved or marked closed, and measures the difference between the Opened and Closed dates. The field is stored in the system as an integer number of seconds.

- On the Incident table, the field is calculated on closure by the business rule mark_closed. The following lines of code calculate the resolve time:

  ```java
  if (dataChange || current.calendar_stc.nil())
      current.calendar_stc = gs.dateDiff(opened, resolved, true);
  ```

- When the incident is closed directly, the calculation is based on the mark_closed business rule. The following lines of code calculate the resolve time:

  ```java
  if (dataChange || current.calendar_stc.nil())
      current.calendar_stc = gs.dateDiff(opened, closed, true);
  ```

Display resolve time as a duration
You can display the resolve time as a human-readable duration rather than an integer representing a duration in seconds.

1. From the Incident or Request form, right-click the form header and click Configure > Table.
2. From the Columns embedded list, click Resolve time.
3. From the Attributes related list, click New.
4. Enter these values.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute</td>
<td>Format</td>
</tr>
<tr>
<td>Dictionary entry</td>
<td>Resolve time</td>
</tr>
<tr>
<td>Value</td>
<td>glide_duration</td>
</tr>
</tbody>
</table>

5. Click Submit.

The resolve time appears in forms and lists as a duration, expressed in days, hours, and minutes.

Note: This attribute does not change the field data format, which remains an integer representing a duration in seconds. In reports and data exports, it still appears as the actual number of seconds, rather than as a duration.

Export date and time formats

Because some export formats are intended for human consumption and others for database usage, various methods are used to provide date and time field information in different formats.

Excel

Date, Date-Time, and Time fields are all exported as their display values, and appear in a custom format, instead of the system date format. However, duration fields, export as the value stored in the database, which is an integer value of seconds.

Note: If the date and time format is \texttt{hh:mm:ss} in the \texttt{glide.sys.date_format} System Properties setting, and you export time values to Excel, they appear in 24-hour military time.

To display the exported values in standard 12-hour am/pm time formats, select the \texttt{1:30PM} time format in Format Cells > Time in Excel.

XML

All Date and Time fields export as the value stored in the database.

PDF

All Date and Time fields (including Duration) export as their display value.
CSV

All Date and Time fields export as the value stored in the database.

Time zones

All times are stored in Coordinated Universal Time (UTC) and appear globally based on the system time zone. However, times appear to users in their local time zone, according to their user preference settings.

Time zone representation

Time zones that have the Country/City format are primary time zone IDs. Other time zone IDs are links to the primary time zone.

- For example, US/Pacific is a link to the America/Los_Angeles time zone. Both America/Los_Angeles and US/Pacific represent Pacific Standard Time with the same zone offset and Daylight Savings Time (DST) schedule.
- Other than the representation, there is no impact on date and time functionality.

In the absence of a default time zone for the user or the system, JVM reads default time zone information from the server.

- Depending on how the server is configured, it might return the Country/City or link, for example, US/Pacific or America/Los_Angeles.
- Administrators should configure their system with a default time zone glide.sys.default.tz to avoid system dependencies. For more information, see Time zone representation.

Daylight Saving Time

In general, if you specify a time zone based on location (for example, America/Los_Angeles), the system automatically adjusts for daylight saving time.

- If you specify a time zone based on the time zone name (for example, GMT), which is discouraged, it does not typically adjust for daylight saving time. There are however exceptions to these guidelines.
- For more detailed information on how daylight saving time is handled in Java, see https://www.iana.org/time-zones and https://en.wikipedia.org/wiki/Tz_database.

User preferences

Once the System Time Zone is defined, users can also select their own time zone from their user form, accessed through Self-Service > My Profile.

- The System default appears as System ([name of the default time zone]).
  
  For example, if the System time zone is America/Los_Angeles, the user sees System (America/Los_Angeles).

Java time zone class

The Now Platform supports all Java time zone class time zones. To view a listing of these time zones:

1. In the Type filter text field, enter sys_user.list.
2. Open one of the user records in the listing.
3. Right-click the time zone field and select Show Choices.
   The resulting list is a complete listing of available time zone IDs.

Java returned for Asian time zone settings

When you set the system date format to HH:mm:ss z to display time zone, and users set their time zone as Asia/Taipei or Asia/Shangai, Java returns the time zone as CST. CST could mean both US Central Standard Time or China Standard time, but in this case, it refers to the latter.

Time zones in email notifications

The date and time stamp of a notification uses the system time zone and not the time zone of any recipient.

- The property glide.email.append.timezone in System Properties > Email controls whether to append the time zone.
  If true, the system time zone of the instance is appended to any dates or date/times in outbound email messages (for example, 2010-07-02 04:01:14 PST).

Time zones in service level agreements

Service level agreements have different options for which time zone to use. To set a time-zone for SLAs, navigate to Service Level Management > SLA Properties and locate the following property:

<table>
<thead>
<tr>
<th>Use the following time zone for SLA:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The caller's time zone</td>
</tr>
<tr>
<td>The caller's time zone</td>
</tr>
<tr>
<td>The SLA definition's time zone</td>
</tr>
<tr>
<td>The CI's location's time zone</td>
</tr>
<tr>
<td>The task's location's time zone</td>
</tr>
<tr>
<td>The caller's location's time zone</td>
</tr>
</tbody>
</table>

Time zone for service level agreements

Some special considerations:

- If you select the time zone for the caller, unpredictable behavior can occur if the caller does not have a time zone defined.
- If you select the time zone for the SLA definition, you must manual specify the time zone on the form for the SLA.

Time zone in scripting

When you create scripting on the server, the script uses several GlideSystem date and time functions to obtain time values. For more information about specific methods and to learn the format in which each returns the requested time, see the GlideSystem API.
Enhancements

DST enhancement requires that reports and queries observe Daylight Saving Time rules. Changes affect trend charts, line charts, and filters using the "trend on" operation.

Time zone changer

The time zone changer is active by default. Users can change their time zone for the current session in the system settings (the gear on the top right of the banner). At the next login, the time zone setting reverts to the system default, or user profile setting for time zone.

Set a system time zone

Set your system time zone with a system property.

The Now Platform stores time values in Universal Coordinated Time. Times appear globally based on the system time zone (glide.sys.default.tz), or if specified, based on user settings.

1. Navigate to System Properties > System.
2. Locate the property System timezone for all users unless overridden in the user’s record [glide.sys.default.tz].

   System timezone for all users unless overridden in the user's record

   By default, the field is blank. If you have not defined a time zone for this property, America/Los Angeles is the default.
3. Add a time zone in the format Country/City or using the name of a time zone (for example, GMT) and click Save. For available values, see Time zone representation.

   The new system time zone automatically cascades to all users who do not already have a specified time zone. If a user selects a different time zone, or if the administrator selects a different time zone for them, the selected time zone is assigned to the user. The system time zone is not used.

Change the time zone choice list

Wherever users have a choice of time zone, the choices are populated using the Time Zone choice list on the User [sys_user] table. Not all time zones appear by default.

To add or remove time zones from the list of time zones:

1. Navigate to User Administration > Users and open any user record, or click New. Notice that the default time zone is System (America/Los_Angeles).
2. Right-click Time zone, and then select Personalize Choices.
3. Highlight the desired time zone from the Available or Selected lists, and then Add or Remove the time zones as needed.
Change a time zone in a scheduled report

By default, scheduled reports use the time zone of the user who runs them (the user in the Run As field) to evaluate the query parameters. You are able to change this time zone.

For example, a report on 'incidents open today' resolves 'today' based on the user's time zone. To manually specify the time zone used to resolve the parameters of the report:

1. Configure the form to add the Run As tz field to the Scheduled Report form.
2. Select the appropriate time zone.

Change a time zone in a scheduled data import

By default, scheduled data imports are run using the time zone of the user who creates them. However, there is a way to manually specify the time zone for the import.

To change the time zone of the scheduled data import:

1. Configure the form to add the Run As tz field to the Scheduled Data Import form.
2. Select the appropriate time zone.
3. Click Update.

Creating business calendars

Create business calendars in the Now Platform so that you can schedule events for your users and track their time across applications. You define schedules and calendars of all types, including fiscal calendars, in the Business Calendar menu.

Business calendar components

Use the following forms when you define calendars and schedules in the Business Calendar menu:

Business calendar definition record

Identifies an individual business calendar where you can specify a reference name, labeling, parent business calendar (if any), and a time zone. A business calendar can represent any time period, and its definition record is saved in the Business Calendar [business_calendar] table. A business calendar can represent any time period, and its definition record is saved in the Business Calendar [business_calendar] table.

To learn more about creating a business calendar definition, see Create a business calendar.

Business calendar entries

Defines the individual entries that make up a business calendar, and saves them in the Business Calendar Entry [business_calendar_span] and Business Calendar Entry Name (business_calendar_span_name) tables. In contrast to legacy schedule entries, which have repeating and excluding time spans, you must create individual business calendar entries for all time spans in the calendar.

To learn more about creating entries for a business calendar, see Define business calendar entries and Create business calendar entry names.

Business calendar filter options

Defines the date and time filtering options for the business calendar that you are creating. These filtering options are in addition to the standard date and time filtering in the Now Platform.

To learn more about creating filtering options for a business calendar, see Create a business calendar.
Calendars for package

Pairs a business calendar with a Now Platform package so that you can enable the calendar for use in that functional area. A package is a collection of scopes and applications that make up a functional area, such as HR Service Delivery.

To learn more about associating a business calendar with a package, see Pair business calendars with packages.

**Warning:** If you are using , use caution when changing time spans. Any change you make to the time span on a business or fiscal calendar can invalidate data. Consult with an administrator before making such changes.

Fiscal calendar example

In this example, you create a fiscal calendar with 4 quarters and 12 fiscal periods.
• When you navigate to Business Calendar > Business Calendars, you create:
  • A business calendar with a title of Fiscal Year.
  • A calendar for quarters that belong to the fiscal year.
  • A calendar for periods with a parent of Fiscal Year or Fiscal Quarter.

When you create the Fiscal Year Quarter child calendar, you designate that the Fiscal Year is its parent calendar. For the child Fiscal Year Period calendar, you designate Fiscal Year Quarter as its immediate parent.

• When you create each calendar, use the Business Calendar Entries related list, or navigate to Business Calendar > Business Calendar Entries to create business calendar entries for it. For each business calendar entry, create a reference name, for example, Fiscal Period 1, and designate start and end date times for each time span within the calendar.
  • For example, the parent Fiscal Year calendar has a business calendar entry for the time span of October 1, 20nn 12:00 a.m. through September 30, 20nn 23:59:59 p.m.
  • The child Fiscal Year Quarter calendar consists of four business calendar entries, each with the start and end dates of each quarter that makes up the fiscal year.

Note: You can also create 13 period, 445, 454 and 544 types of fiscal calendars. To learn more about these types of fiscal calendars, see Defining fiscal calendars.

• The child Fiscal Year Quarters calendar consists of multiple business calendar entries, with the start and end date times for each period in the fiscal year.

• Use Business Calendar > Calendars for Package to pair the parent Fiscal Year 20nn calendar with Now Platform packages, such as HR Service Delivery or Finance Close Automation.

Business calendar schedule example

In this example, you create a work schedule for the month of December.

• The work schedule consists of a parent calendar, a child calendar for the working weeks in December, and another child calendar for the working days in December.
• The December Workdays calendar consists of business calendar entries for each working day. You do not include non-work days such as Saturdays, Sundays, and company holidays.
• Use Business Calendar > Business Calendars to create a parent business calendar with a title of December Work Schedule, and a child business calendar for December work weeks. When you create the child calendar, you designate that the December Work Schedule is its parent calendar.

Note: You can make the December Work Schedule even more granular by creating a subordinate child calendar for December workdays. In this case, its immediate parent is the December Work Weeks calendar.

• When you create each calendar, use the Business Calendar Entries related list, or navigate to Business Calendar > Business Calendar Entries to create at least one business calendar entry for it. For each business
calendar entry, you give it a reference name, and designate the start and end date times for each time span within
the calendar.

- For example, the parent December Work Schedule calendar is for a time span of December 1, 20nn 12:00 a.m.
  through December 31, 20nn 23:59:59 p.m.
- The child December Work Week calendar consists of five business calendar entries. Each entry is for the start
  and end dates of each calendar week in December.
- The child December Workdays calendar consists of multiple business calendar entries. Each entry is for the
  start and end date times for each working day in December. You do not create business calendar entries for
  company holidays such as New Year's Eve or New Year's Day.

- Use Business Calendar > Calendars for Package to pair the parent business calendar December Work
  Schedule with the appropriate Now Platform packages, such as Customer Service Management.

Using business calendars in place of legacy calendar and schedule definitions

The legacy functions that you may have used, on the System Scheduler > Schedules and Fiscal Calendar menus,
to define schedules and fiscal calendars, continue to be supported. However, you should use the Business Calendar
menu in their places to define calendars and schedules and then associate them with specific Now Platform packages.

- If you use the legacy functions to create fiscal calendars and schedules, the resulting definition records are
  internally flagged as belonging to the legacy [cmn_schedule] table hierarchy. These records appear on the lists
  on the Business Calendar menu, as well as on the lists on the respective menus for the legacy functions used. For
  example, if you defined fiscal calendars using legacy fiscal calendar functions, the resulting records appear on lists
  on the Business Calendar Fiscal Calendar menus.
- If you select a legacy fiscal calendar or schedule from these lists, you can only modify it using the legacy function
  that you originally used to create it. For example, if you select a legacy fiscal calendar, you can only modify it by
  using the functions on the Fiscal Calendar menu. You can't modify it with the Business Calendar menu functions.

Create a business calendar

Create a definition record for an individual parent or child business calendar. You create this record so that you can
easily identify a specific business calendar when you use it in a Now Platform package or functional area. A business
calendar can represent any length of time, such as a week, a month, a year, or a fiscal period.

Role required: admin

When you create a business calendar, you specify a reference name, labeling, parent business calendar, if any, and a
time zone for it.

1. You first create a business calendar record and then create business calendar entries for it in the Business
   Calendar Entries related list. To learn more about how business calendar entries work, see Define business
   calendar entries and Create business calendar entry names.

2. Using the Business Calendar Filter Options related list, you can also define the date and time filtering options for
   the business calendar that you are creating.

Note: Fiscal calendars or schedules you may have created in the Fiscal Calendar or System
Scheduler > Schedules menu also appear on the lists on the Business Calendar menu. If you select a
fiscal calendar or schedule, it appears in the legacy function that you originally used to create it. You can't
view or update legacy fiscal calendars or schedules using this form.

1. Navigate to Business Calendar > Business Calendars.
2. Click New.
3. On the form, fill in the fields.

**Business calendar form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique reference name and identifier for the business calendar record. The name should be unique per domain.</td>
</tr>
<tr>
<td>Label</td>
<td>Unique singular label for identifying the business calendar when you perform filtering. For example, you can assign a week-long work calendar with a label of Workweek.</td>
</tr>
<tr>
<td>Plural Labels</td>
<td>Unique plural label for identifying the business calendar. For example, you can assign a week-long work calendar with a label of Workweeks. Use plural labels when you do filtering that is based on more than one unit in the past or future. For example, Last 2 Fiscal Quarters.</td>
</tr>
</tbody>
</table>
| Parent         | Parent business calendar to the current business calendar that you are creating. To search for an existing business calendar, click

  - For example, you created a business calendar for 2020, and an individual child calendar for each month within the year, each with its own business calendar entries. As you create a business calendar for each month, you would select 2020 as the parent calendar for each.

  - These entries create the relationship between a parent and its child business calendars. Leave this field blank if you are creating a parent business calendar itself. |
| Application    | Application that is associated with this business calendar. If you are working on an application or are creating a business calendar from an application record, the field defaults to that application. Otherwise, the field defaults to Global. Any records that are created from the table record, such as modules and security rules, are assigned to this application by default. To learn more about application scoping, see Application scope |
### Time zone

Time zone to use for the business calendar when you specify the starting and ending times for each associated business calendar entry. Select a time zone entry:

- **-None-**: Use the time zone specified in the logged in user's profile.
- **Use System Time Zone**: Use the default system time zone specified for the instance.
- **- Floating --**: Time zone is relative to whatever is accessing the business calendar entry at any given time. For example, if an administrator in Amsterdam creates a floating business calendar for 08:00 a.m. to 5:00 p.m., a person in San Jose, California, sees it as 08:00 a.m. to 5:00 p.m. When you define a business calendar in a specific time zone, users in different time zones see the business calendar in their own time zone.
- **Actual time zone. For example, Europe/London, US/Pacific, US/Central.**

### Description

Description of the business calendar.

---

4. Click **Submit**.
5. In the Business Calendars list, select the business calendar that you created.
6. In the Business Calendar Entries related list, create entries that define each span of time within the business calendar.

Create at least one business calendar entry for the selected calendar.

**Note:** To learn more about creating business calendar entries, see [Define business calendar entries](#) and [Creating business calendars](#).

7. In the Business Calendar Filter Options related list, click **New** to create filtering options for the business calendar.

You can define the date and time filtering options for the business calendar that you are creating. These filtering options are in addition to the standard date and time filtering in the Now Platform.

**Note:** To learn more about creating business calendar filtering options, see [Define business calendar filtering options](#).

8. Click **Submit**.

A business calendar record is saved in the Business Calendar [business_calendar] table.

- If you create business calendar entries in the Business Calendar Entries related list, records are created in the Business Calendar Entry (business_calendar_span) table. The records are associated with the business calendar.
- If you created business calendar filter options in the Business Calendar Filter Options related list, a record is saved in the Business Calendar Filter Option (business_calendar_filter_option) table. The record is associated with the business calendar.
Create a business calendar group

For Performance Analytics and Reporting to use business calendars, organize several calendars into a business
calendar group. An application might also contain a business calendar group.

You can base a Performance Analytics indicator or a report on business calendars instead of the standard calendar.
The business calendars themselves are too granular in scale, and have to be grouped. The report or indicator then uses
that group. Work with your Performance Analytics team to design the business calendar groups.

Note: Fiscal calendars are also supported. When you generate a fiscal calendar, a corresponding business
calendar group is also generated automatically.

Role required: admin

1. Navigate to Business calendars > Business calendar group.
2. Select New.
3. Name the group and save it.
   The Business calendars related list appears.
4. In the Business calendars related list, select Edit.
5. Choose from existing business calendars to add to the group.
   You can also create a new business calendar from this list.

   Important: Do not select business calendars that cover a period shorter than a 24-hour day for use with
   Performance Analytics indicators. Performance Analytics does not store times, only dates. If only reports
   will use the group, you can select a shorter period.

6. Select Update when finished.

Gregorian calendar group

The Gregorian Calendar group comes with the base system. It includes the Week, Month, Quarter, and Year business
calendars, which also come with the base system.
## Business Calendar Group

**Gregorian calendar**

<table>
<thead>
<tr>
<th>Application (ID)</th>
<th>Name</th>
<th>Description</th>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Gregorian calendar</td>
<td>Gregorian calendar</td>
<td>global</td>
</tr>
</tbody>
</table>

### Business Calendars

<table>
<thead>
<tr>
<th>Business calendar</th>
<th>Order</th>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Week</td>
<td>100</td>
<td>global</td>
</tr>
<tr>
<td>Month</td>
<td>200</td>
<td>global</td>
</tr>
<tr>
<td>Quarter</td>
<td>300</td>
<td>global</td>
</tr>
<tr>
<td>Year</td>
<td>400</td>
<td>global</td>
</tr>
</tbody>
</table>

Actions on selected rows...
Each business calendar record also shows which groups it belongs to.
Define business calendar entries

Create business calendar entry records that define the individual time periods that make up a business calendar. You create a business calendar entry for every individual time span in the calendar.

Role required: admin

In contrast to legacy schedule entries that have repeating and excluding time spans, you have to create individual business calendar entries for every business calendar time span. For example, if you are creating a Fiscal Year 2020 business calendar with 13 fiscal periods, you have to create individual business calendar entries for each fiscal period. For each fiscal period, you specify start and end date times.

**Note:** Fiscal calendars or schedules you may have created in the Fiscal Calendar or System Scheduler > Schedules menu also appear on the lists on the Business Calendar menu. If you select a fiscal calendar or schedule, it appears in the legacy function that you originally used to create it. You can't view or update legacy fiscal calendars or schedules using this form.

**Note:** The easiest way to create business calendar entries and associate them with a business calendar is to use the Business Calendar Entries related list in the Business Calendar form. To learn more about creating a business calendar, see Create a business calendar.

1. Navigate to Business Calendar > Business Calendar Entries.
2. Click New.
3. On the form, fill in the fields.

### Business calendar entry form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Name      | Unique reference name for the business calendar entry. To select a business calendar name or create a new one:  
  a. To search for an existing business calendar entry name, click  
  
  b. If no business calendar entry name exists and you want to create a new business calendar entry name, click New. The Business Calendar Entry Name form appears.  
  
  **Note:** To learn how to create business calendar entry names, see Create business calendar entry names. |
| Start     | Start date and time for the business calendar period. It uses the time zone that you specified in the business calendar record that you associate with it. For example, if you are defining a fiscal period for the month of January, the starting date time is January 31, 2020 12:00 a.m. |
4. Click Submit.

Create business calendar entry names

Create a name for an individual business calendar entry. You create this record so you can easily identify a specific business calendar entry when you use it in a business calendar.

Role required: admin

1. Navigate to Business Calendar > Business Calendar Entry Names.

   Note: Alternately, you can create a business calendar entry name at the time you create the associated business calendar entry. To learn more about creating a business calendar entry, see Define business calendar entries.

2. Click New.
3. On the form, fill in the fields.

   Business calendar entry name form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short name</td>
<td>Abbreviated name for the business calendar entry. For example, January.</td>
</tr>
<tr>
<td>Long name</td>
<td>Longer name for the business calendar entry. For example, January fiscal period.</td>
</tr>
<tr>
<td>Label</td>
<td>Unique label for identification of the business calendar entry when you perform filtering.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Calendar | Name of the business calendar that you want the business calendar entry to belong to. This entry creates the relationship between a business calendar and the business calendar entries that define each individual time span with it. For example, if you are creating a business calendar entry for the January fiscal period, you select FY20 to associate it with Fiscal Year 2020. To select an existing business calendar:  
   a. Click or  
   b. Click inside the Calendar field to view and select from a listing of recent business calendars that are created in Business Calendar > Business Calendars. |
| Application | Application that is associated with this business calendar. If you are working on an application or are creating a business calendar from an application record, the field defaults to that application. Otherwise, the field defaults to Global. Any records that are created from the table record, such as modules and security rules, are assigned to this application by default. To learn more about application scoping, see Application scope. |

4. Click **Submit**.

Records are created in the Business Calendar Entry (business_calendar_span) and the Business Calendar Entry Name (business_calendar_span_name) tables. If you create business calendar entries in the Business Calendar Entries related list in the Business Calendar form, these records are also associated with the specific business calendar.

**Define business calendar filtering options**

Define date and time filtering options for a business calendar. These filtering options are in addition to the standard date and time filtering in the Now Platform. You can provide your users with additional filtering options when they use the business calendar with Now Platform packages and functional areas.

Role required: admin

To learn more about standard filtering options, see Values for date/time fields.
1. Navigate to Business Calendar > Business Calendar Filter Options.
2. Click New.
3. On the form, fill in the fields.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Period</td>
<td>Number of periods that should be traversed forward, backward, or both, for the business calendar. For example, if the business calendar reflects a week:</td>
</tr>
<tr>
<td></td>
<td>• Provide a filter option for the current week by entering 0 for the base period.</td>
</tr>
<tr>
<td></td>
<td>• Provide a filter option for a previous period by entering a negative number that represents the number of periods that should be traversed from the base period. For example, enter −1 for the last period, or enter −2 for two periods ago.</td>
</tr>
<tr>
<td></td>
<td>• Provide a filter option for a future period by entering a positive number. For example, enter 1 for the next period, or enter 2 for the next two weeks.</td>
</tr>
</tbody>
</table>

If the business calendar reflects a week:

• Provide a filter option for the current week by entering 0 for the base period.

• Provide a filter option for a previous period by entering a negative number that represents the number of periods that should be traversed from the base period. For example, enter −1 for the last period, or enter −2 for two periods ago.

• Provide a filter option for a future period by entering a positive number. For example, enter 1 for the next period, or enter 2 for the next two weeks.

If the business calendar reflects a fiscal year with 13 periods:

• Provide a filter option for the current fiscal year by entering 0 for the base period.

• Provide a filter option for a previous fiscal year by entering a negative number that represents the number of periods that should be traversed from the base period. For example, enter −2 for two fiscal periods ago, or enter −13 for the last fiscal year.

• Provide a filter option for a future fiscal year by entering a positive number. For example, enter 13 for the next fiscal year.

If the business calendar reflects a fiscal year with four fiscal quarters:

• Provide a filter option for the current fiscal quarter by entering 0 for the base period.

• Provide a filter option for a previous fiscal quarter by entering a negative number that represents the number of periods that should be traversed from the base period. For example, enter −1 for the last fiscal quarter, or enter −2 for the last two fiscal quarters.

• Provide a filter option for a future fiscal quarter by entering a positive number. For example, enter 1 for the next fiscal quarter, or enter 2 for the next two fiscal quarters.
## Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calendar</td>
<td>Name of the business calendar that you want the filter options to belong to.</td>
</tr>
<tr>
<td></td>
<td>To select a business calendar, or create a new one:</td>
</tr>
<tr>
<td></td>
<td>a. Search for an existing business calendar by clicking</td>
</tr>
<tr>
<td></td>
<td>b. If no business calendar exists, or if you want to create a new business calendar, click <strong>New</strong>.</td>
</tr>
<tr>
<td>Application</td>
<td>Application that is associated with this business calendar.</td>
</tr>
<tr>
<td></td>
<td>If you are working on an application or are creating a business calendar from an application record, the field defaults to that application. Otherwise, the field defaults to <strong>Global</strong>. Any records that are created from the table record, such as modules and security rules, are assigned to this application by default. To learn more about application scoping, see <strong>Application scope</strong>.</td>
</tr>
</tbody>
</table>

**Note:** Within a calendar filtering option record, you can only associate a business calendar with a single filter option. To create multiple filtering options, you have to create multiple filtering option records, each with its own period entry.

4. Click **Submit**.

Records are created in the Business Calendar Filter Option (business_calendar_filter_option) table. If you create business calendar filtering options in the Business Calendar Filter Options related list in the Business Calendar form, these records are also associated with the specific business calendar.

### Pair business calendars with packages

Pair a business calendar that you created with a package, or functional area, in the Now Platform. When you associate a business calendar with a package, it enables the use of the calendar in that specific functional area. Until you pair a business calendar definition with at least one package, it remains a definition record only.

Role required: admin

A package is an application, or generic set of functions, such as HR Service Delivery or Finance Close Automation, in the Now Platform. For example, if you created a fiscal calendar, you can associate it with the Finance Close Automation package.

**Note:** Within a single calendar package record, you can only associate a business calendar with a single package. To associate business calendars with multiple packages, you have to create multiple calendar package records. For example, if you created a fiscal calendar and want to associate it with the HR and Fixed Assets packages:

- In the first record you create, in the **Calendar** field, select the fiscal year, and in the **Package** field, select **HR**.
1. Navigate to Business Calendar > Calendars for Package.
2. Click New.
3. On the form, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calendar</td>
<td>Name of the business calendar that you want to associate with a Now Platform package. Click to access Business Calendars where you can search for an existing business calendar. If there is no existing calendar, you can create a new one.</td>
</tr>
<tr>
<td>Package</td>
<td>Name of the Now Platform package that you want to associate with the selected business calendar. Click to access Packages where you can search for an existing package. If there is no existing package, you can create a new one.</td>
</tr>
</tbody>
</table>

4. Click Submit.

A record is created in the Calendars for Package (calendars_for_package) table that associates the selected business calendar with a Now Platform package.

**Defining fiscal calendars**

Create fiscal calendars with defined fiscal periods, for use with Financial Management applications, such as Finance Close Automation. You can define fiscal periods, such as one month long, four weeks long, Q1 2015, or July 2015.

To create a fiscal calendar, activate the Fiscal Calendar [com.snc.fiscal_calendar] plugin. You can then use the legacy functions on the Fiscal Calendar menu to generate and validate fiscal calendars and their associated fiscal periods. You can create one of these types:

<table>
<thead>
<tr>
<th>Calendar type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regular</td>
<td>A calendar with 12 periods, each of which is one month long.</td>
</tr>
<tr>
<td>13 Period</td>
<td>A calendar with 13 periods, each of which is four weeks long.</td>
</tr>
<tr>
<td>445</td>
<td>A calendar that divides a year into subsequent 4-week, 4-week, 5-week periods. The first and second periods have four weeks, and the last has five weeks. The application creates these periods for the calendar duration.</td>
</tr>
</tbody>
</table>

*Note:* This calendar is the only type that does not use quarters.
Calendar type | Description
--- | ---
454 | A calendar that divides a year into subsequent 4-week, 5-week, 4-week periods. The first period has four weeks, the second has five weeks, and the third has four weeks. The application creates these periods for the calendar duration.

544 | A calendar that divides a year into subsequent 5-week, 4-week, 4-week periods. The first period has five weeks, and the second and third have four weeks.

**Attention:** Once you start working with a set of financial data with a fiscal calendar type, you cannot change to another type of fiscal calendar. Verify that your fiscal calendar can be used with your financial data. If you import records into the Fiscal period [fiscal_period] table, you should validate that they are correct and do not contain any gaps.

**Note:** The legacy functions that you may have used, on the System Scheduler > Schedules and Fiscal Calendar menus, to define schedules and fiscal calendars, continue to be supported. However, you should use the Business Calendar menu in their places to define calendars and schedules and then associate them with specific Now Platform packages. To learn more about defining and using business calendars, see Creating business calendars.

**Activate Fiscal Calendar plugin**

If you have the admin role, you can activate the Fiscal Calendar plugin (com.snc.fiscal_calendar). This plugin includes demo data and activates related plugins if they are not already active.

Role required: admin

1. Navigate to System Applications > All Available Applications > All.
2. Find the plugin using the filter criteria and search bar.
   
   You can search for the plugin by its name or ID. If you cannot find a plugin, you might have to request it from ServiceNow personnel. For more information, see Request a plugin.
3. Click Install, and then in the Activate Plugin dialog box, click Activate.

**Note:** When domain separation and delegated admin are enabled in an instance, the administrative user must be in the global domain. Otherwise, the following error appears: Application installation is unavailable because another operation is running: Plugin Activation for <plugin name>.

**Generate a fiscal calendar**

You can generate a fiscal calendar for a specified time period.

Role required: fiscal_calendar_admin

**Attention:** Once you start working with a set of financial data with a fiscal calendar type, you cannot change to another type of fiscal calendar. Verify that your fiscal calendar can be used with your financial data.
Note: Instead of generating fiscal calendars, can also use the Business Calendar functions to create fiscal calendars. To learn more about creating business calendars, see Creating business calendars.

1. Navigate to Fiscal Calendar > Generate
2. Configure the form (see table).
3. Click Generate Calendar.
4. Navigate to System Definition > Fiscal Periods and verify that the monthly, quarterly, and annual fiscal period records exist.

### Fiscal Calendar Types

<table>
<thead>
<tr>
<th>Standard</th>
<th>13 Periods</th>
<th>445</th>
</tr>
</thead>
<tbody>
<tr>
<td>Year</td>
<td>Year</td>
<td>Year</td>
</tr>
<tr>
<td>4 Quarters</td>
<td>13 Periods</td>
<td>4 Quarters</td>
</tr>
<tr>
<td>12 Months</td>
<td></td>
<td>12 Periods</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fiscal Calendar Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fiscal Unit</td>
</tr>
<tr>
<td>Start Month</td>
</tr>
<tr>
<td>Start Year</td>
</tr>
<tr>
<td>Prefix for Year</td>
</tr>
<tr>
<td>Prefix for Quarter</td>
</tr>
<tr>
<td>Start Day</td>
</tr>
<tr>
<td>End Year</td>
</tr>
<tr>
<td>Prefix for Period</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fiscal Calendar Types</td>
<td>Type of fiscal year calendar. Select the type of calendar by clicking it. The options in the lists update automatically.</td>
</tr>
<tr>
<td>Fiscal Unit</td>
<td>Base unit for the calendar.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Month</strong>: Generate fiscal calendar with monthly periods.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Quarter</strong>: Generate fiscal calendar with quarterly periods.</td>
</tr>
</tbody>
</table>
### View, modify, and validate fiscal periods

After you generate a fiscal calendar, you can view fiscal period records, modify the start and end date, deactivate a fiscal period if necessary, and validate.

Role required: fiscal_calendar_user

1. Navigate to **System Definition > Fiscal Periods**.
2. Open any of the fiscal periods (see table for field descriptions) to view, modify, or deactivate.

<table>
<thead>
<tr>
<th>Fiscal period form</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the fiscal period.</td>
</tr>
<tr>
<td>Start date time</td>
<td>Date the fiscal period starts.</td>
</tr>
<tr>
<td>End date time</td>
<td>Date the fiscal period ends.</td>
</tr>
<tr>
<td>Fiscal Type</td>
<td>[Read-Only] Type of period, either <strong>Year</strong> or <strong>Quarter</strong>.</td>
</tr>
</tbody>
</table>

3. Validate the fiscal periods to ensure that there are no gaps and that they match a valid style of calendar.
   a) To validate, return to the list view of fiscal periods and click **Validate Periods**.

### Creating and using schedules

Use schedules to specify when service level agreements or inactivity monitors are active, or to specify when on-call rotations should take effect. Schedules are rules that include or exclude time for various actions or tasks.

For example, if a service level agreement is set to an 8-5 Weekdays schedule, the SLA only counts time during those hours. Generate and validate schedules in the **System Scheduler > Schedules** menu.

**Note:** The legacy functions that you may have used, on the **System Scheduler > Schedules** and Fiscal Calendar menus, to define schedules and fiscal calendars, continue to be supported. However, you should use the Business Calendar menu in their places to define calendars and schedules and then associate them with specific Now Platform packages. To learn more about defining and using business calendars, see Creating business calendars.
Default schedules

Default schedules are available in a base system.

<table>
<thead>
<tr>
<th>Name</th>
<th>Schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>8-5 weekdays</td>
<td>Repeats every week on weekdays Monday through Friday.</td>
</tr>
<tr>
<td>8-5 weekdays excluding holidays</td>
<td>Repeats every week on weekdays Monday through Friday. Includes the child schedule U.S. Holidays.</td>
</tr>
<tr>
<td>Application</td>
<td>Repeats every week on Sunday.</td>
</tr>
<tr>
<td>Application FLX</td>
<td>Repeats every week on Sunday.</td>
</tr>
<tr>
<td>Blackout Wednesdays (GMT)</td>
<td>Repeats every week on Wednesday.</td>
</tr>
<tr>
<td>Database Server FLX</td>
<td>Repeats every week on Saturday.</td>
</tr>
<tr>
<td>Default MS Project</td>
<td>Repeats every week on weekdays Monday through Friday from 8:00am to noon and 1:00-5:00pm. Default schedule for the Project Management application.</td>
</tr>
<tr>
<td>Global Infrastructure</td>
<td>Repeats every week on Saturday.</td>
</tr>
<tr>
<td>MySQL Database Service</td>
<td>Repeats every week on Saturday.</td>
</tr>
<tr>
<td>Network</td>
<td>Repeats every week on Saturday.</td>
</tr>
<tr>
<td>Project Management Schedule</td>
<td>Repeats every week on weekdays Monday through Friday from 8:00am to noon and 1:00-5:00pm. Default schedule for the Project Management application.</td>
</tr>
<tr>
<td>Resource Management Schedule</td>
<td>Repeats every week on weekdays Monday through Friday from 8:00am to noon and 1:00-5:00pm. Default schedule for the Resource Management application.</td>
</tr>
<tr>
<td>Server</td>
<td>Repeats every week on Saturday.</td>
</tr>
<tr>
<td>Servers San Diego</td>
<td>Repeats every week on Wednesday.</td>
</tr>
<tr>
<td>Software Blackout</td>
<td>Repeats every week on Wednesday.</td>
</tr>
<tr>
<td>WebServer FLX</td>
<td>Repeats every week on Sunday.</td>
</tr>
<tr>
<td>Weekends</td>
<td>Repeats every week on Saturday for two days.</td>
</tr>
</tbody>
</table>

Holidays

You can define each individual holiday as a schedule entry to create exceptions to existing schedules.

For instance, if an SLA requires an incident be resolved within three business days excluding Christmas, create a schedule entry for Christmas. Creating this entry ensures that the SLAs do not count Christmas when calculating elapsed time, even if it falls within the work week.

Because schedules can be included in other schedules through a parent-child relationship, it is also possible to create a holiday schedule and include it in other schedules to keep holidays consistent. The following example shows a holiday schedule.
### Schedule - U.S. Holidays

<table>
<thead>
<tr>
<th>Name</th>
<th>Starts</th>
<th>Ends</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Christmas Day</td>
<td>Every year on Dec 25</td>
<td>12-25-2012 00:00:00</td>
<td>12-25-2012 23:59:59</td>
</tr>
<tr>
<td>Christmas Eve</td>
<td>Every year on Dec 24</td>
<td>12-24-2012 00:00:00</td>
<td>12-24-2012 23:59:59</td>
</tr>
<tr>
<td>Columbus Day</td>
<td>Every year on 2nd Mon of Oct</td>
<td>10-09-2012 00:00:00</td>
<td>10-09-2012 23:59:59</td>
</tr>
<tr>
<td>Independence Day</td>
<td>Every year on July 4</td>
<td>07-04-2012 00:00:00</td>
<td>07-04-2012 23:59:59</td>
</tr>
<tr>
<td>Labor Day</td>
<td>Every year on 1st Mon of Sep</td>
<td>09-01-2012 00:00:00</td>
<td>09-01-2012 23:59:59</td>
</tr>
<tr>
<td>Martin Luther King, Jr. Day</td>
<td>Every year on 3rd Mon of Jan</td>
<td>01-16-2012 00:00:00</td>
<td>01-16-2012 23:59:59</td>
</tr>
<tr>
<td>Memorial Day</td>
<td>Every year on last Mon of May</td>
<td>05-28-2012 00:00:00</td>
<td>05-28-2012 23:59:59</td>
</tr>
<tr>
<td>New Year's Day</td>
<td>Every year on Jan 1</td>
<td>01-01-2012 00:00:00</td>
<td>01-01-2012 23:59:59</td>
</tr>
<tr>
<td>New Year's Eve</td>
<td>Every year on Dec 31</td>
<td>12-31-2012 00:00:00</td>
<td>12-31-2012 23:59:59</td>
</tr>
<tr>
<td>Presidents' Day</td>
<td>Every year on 3rd Mon of Feb</td>
<td>02-20-2012 00:00:00</td>
<td>02-20-2012 23:59:59</td>
</tr>
<tr>
<td>Thanksgiving Day</td>
<td>Every year on 4th Thu of Nov</td>
<td>11-22-2012 00:00:00</td>
<td>11-22-2012 23:59:59</td>
</tr>
<tr>
<td>Veterans Day</td>
<td>Every year on Nov 11</td>
<td>11-11-2012 00:00:00</td>
<td>11-11-2012 23:59:59</td>
</tr>
</tbody>
</table>
The following example shows a schedule that includes the preceding holiday schedule.

Child Schedule
Create a holiday schedule for multiple regions

You can create holiday schedules for multiple regions that follow the same work schedule but have different holidays.

The following method supports multiple regions with the same work schedule (for example, an 8-5 weekdays schedule) but with different holiday schedules.

1. Create a holiday schedule for each region. For example, U.S. Holidays, British Holidays, and Australian Holidays.
2. Add the work schedule as a child schedule to each region's holiday schedule.

This method requires making \(<\text{number of schedules}\> + 1\) total schedules. If you make the regional holiday schedule a child schedule of the work hours schedule, you must create a separate work hours schedule for each region. The total number of schedules in this case is \(<\text{number of schedules}\> \times 2\) schedules.

Parent and child schedules

Schedules can have one of two parent-child relationships with other schedules.

Parent field

When a schedule record lists a value for the Parent field, schedule entries from the parent schedule apply to both the parent schedule and the child schedule. By default, there are no sample schedules that use the Parent field.

Child schedule

When a schedule record has one or more child schedules in the Child Schedules related list, schedule entries from the child schedule apply to the containing schedule. By default, there are several sample schedules that use child schedules. For example, see the 8-5 weekdays excluding holidays schedule that includes the U.S. Holidays schedule.

Parent and child schedules cannot contain conflicting schedule entry types. For example, a schedule containing maintenance schedule entries cannot also contain blackout schedule entries. Nor can a maintenance schedule have a child schedule containing blackout schedule entries.

Note: To create a Holiday schedule and include it in a parent schedule, you must add it as a child schedule and with an Include type.

Parent schedules must have at least one entry that is not an Excluded type. If parent schedules are only exclusionary, they are invalid.

Note: The Show Schedule related link shows schedule entries from the current schedule and the child schedule record. For example, when showing the 8-5 weekdays excluding holidays schedule, holidays are also shown as excluded because the holiday schedule is a child schedule.

Define a schedule

You configure schedules using schedule and schedule entry records.

- Schedule records specify a time zone and a type of schedule and use one or more schedule entries. Schedule records are saved in the Schedule [cmn_schedule] table.
- Schedule entry records specify the time periods that are included or excluded from a schedule. Schedule entries are saved in the Schedule Entry [cmn_schedule_span] table.
1. Navigate to **System Scheduler > Schedules > Schedules**.
2. Click **New**, enter a unique and meaningful **Name** and **Description** and then fill in the form.
   For detailed information on Schedule form fields, see **Schedule fields**.

   **Note:** If there are no active entries defined for the current schedule, a warning message appears in the Schedule form. If your schedule is a child schedule that contains only exclusions, ignore the message because exclusions are non-active entries.

3. Right-click the header bar and click **Save**.

   **Note:** If you create a schedule of type **maintenance** and save the record, a UI policy hides the **Type** field from the form. To view or change the **Type** value, use the list of schedules instead of the schedule form. Add the **Type** column if necessary. You can click the cell for the value in the **Type** column and modify the value in the list view.
4. Configure one or more schedule entries.
   For detailed information on Schedule Entry form fields, see Schedule entry fields.
## Schedule

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>8-5 weekdays</td>
</tr>
<tr>
<td>Time zone</td>
<td>-- Floating --</td>
</tr>
<tr>
<td>Parent</td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>Global</td>
</tr>
<tr>
<td>Type</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
</tbody>
</table>

### Related Links

#### Schedule

<table>
<thead>
<tr>
<th>Schedule Entries</th>
<th>Child Schedules</th>
<th>Referenced By</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Schedule Entries

- **Monday-Friday 8-5:** Weekly on Weekdays, 1
  - Start date time: 2008-07-07 08:00:00
  - End date time: 2008-07-07 17:30:00

Actions on selected rows...
Schedule fields

The Schedule form contains the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name for the schedule.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>Time zone for the schedule. If you select <strong>Floating</strong>, the time zone is relative to whatever process is accessing the item at the time.</td>
</tr>
<tr>
<td></td>
<td>• For example, if a resource manager in Amsterdam sets a floating schedule for 8:00 A.M. to 5:00 P.M., a user in San Jose sees the schedule as 8:00 A.M. to 5:00 P.M.</td>
</tr>
<tr>
<td></td>
<td>• When a schedule is defined in a specific time zone, users in different time zones see the schedule with their own time zone applied.</td>
</tr>
<tr>
<td>Parent</td>
<td>Parent schedule that constraints the new schedule.</td>
</tr>
<tr>
<td>Application</td>
<td>Application scope of the schedule.</td>
</tr>
<tr>
<td>Type</td>
<td>Text label that describes the purpose of the schedule. You can also use one of these system terms to determine how to process certain schedules:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Excluded</strong>: Excludes time periods from SLA counts.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Maintenance</strong>: Specifies time periods where change management activities are allowed. A schedule containing maintenance schedule entries cannot also contain blackout schedule entries.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Blackout</strong>: Excludes time periods from change management schedules. A schedule containing blackout schedule entries cannot also contain maintenance schedule entries.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the schedule.</td>
</tr>
</tbody>
</table>

Schedule entry fields

You can only associate a schedule entry with one schedule. The **Schedule Entries** related list contains the definitions of the time periods you want to include in or exclude from the schedule.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name for the schedule entry.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Label that describes the purpose of the schedule. The system also uses the schedule type to determine how to process certain schedules.</td>
</tr>
<tr>
<td>• <strong>Excluded</strong>: Excludes time periods from SLA counts.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Maintenance</strong>: Specifies time periods where change management activities are allowed. A schedule containing maintenance schedule entries cannot also contain blackout schedule entries.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Blackout</strong>: Excludes time periods from change management schedules. A schedule containing blackout schedule entries cannot also contain maintenance schedule entries.</td>
<td></td>
</tr>
<tr>
<td><strong>Show As</strong></td>
<td>Option that indicates how the schedule entry should appear in calendar applications and how it should interact with other schedule entries.</td>
</tr>
<tr>
<td>• <strong>Busy</strong>: Schedule entry is not available for scheduling a work task.</td>
<td></td>
</tr>
<tr>
<td>• <strong>At no extra charge</strong>: Schedule entry is available for scheduling a work task.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Tentative</strong>: Schedule entry is tentatively available for scheduling a work task.</td>
<td></td>
</tr>
<tr>
<td>• <strong>On call</strong>: Schedule entry is on call, which provides a means to determine which member of a user group is available to complete a task.</td>
<td></td>
</tr>
<tr>
<td><strong>When</strong></td>
<td>Date and time to which the schedule entry applies. If the schedule entry applies to a full 24-hour day, select the <strong>All day</strong> check box.</td>
</tr>
<tr>
<td><strong>Note</strong>: Changing the global date and time format in the <code>glide.sys.date_format</code> System Properties setting has significant impact on schedule calculations made when you select the <strong>All day</strong> check box. To learn more, see Global date and time field format.</td>
<td></td>
</tr>
<tr>
<td><strong>Repeats</strong></td>
<td>Repetition interval for the schedule entry, if any. If you select a repetition interval, other fields appear so you can further specify the repeat interval.</td>
</tr>
<tr>
<td><strong>Repeat every</strong></td>
<td>Scheduling repetition frequency - weekly, monthly, or yearly. This field is only visible when the <strong>Repeats</strong> field has a value of <strong>Daily</strong>, <strong>Weekly</strong>, <strong>Monthly</strong>, or <strong>Yearly</strong>.</td>
</tr>
<tr>
<td><strong>Repeat on</strong></td>
<td>Days of the week a weekly schedule repeats on. This field is only visible when the <strong>Repeats</strong> field has a value of <strong>Weekly</strong>.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Monthly type | Monthly schedule repetition frequency. This field is only visible when the Repeats field has a value of Monthly. Monthly repeat options include:  
• Repeat on a specific day of the month  
• Repeat on a specific day in a specific week of the month  
• Repeat on the last day of the month  
• Repeat on a specific weekday in the last week of the month |
| Yearly type | Yearly schedule repetition frequency. This field is only visible when the Repeats field has a value of Yearly. Yearly repeat options include:  
• Repeat on a specific day of the year  
• Repeat on a floating day |
| Float week | Week of the month a floating yearly schedule repeats on. This field is only visible when the Yearly type field has a value of Floating. |
| Float day | Day of the week a floating yearly schedule repeats on. This field is only visible when the Yearly type field has a value of Floating. |
| Month | Month of the year a floating yearly schedule repeats on. This field is only visible when the Yearly type field has a value of Floating. |
| Repeat until | Repetition end date. If you leave this field blank, the schedule repeats indefinitely. |
| Type | [Optional] Schedule entry description. |

**Schedule for the fifth instance of a week date**

You can select a date that computes to the fifth instance of a weekday for a date near the end of a month for a repeating monthly schedule,

Three options are available for handling months that do not have a matching Fifth instance of the selected day.

- Last: Selects the last instance of the weekday in the month.  
- Next: Selects the first instance of the weekday in the next month.  
- Strict: Skips any month without a matching Fifth instance and selects only months that have a matching Fifth instance.

Use the `glide.schedules.fifth` system property to control how a schedule entry that selects the fifth occurrence of a weekday behaves in months containing only four occurrences of that day.

- Use of this property is only valid when the `glide.schedules.repeat_nth` property is set to Day.  
- The following example illustrates computing what day of the month a schedule repeats on when the schedule starts on the Fifth instance of a weekday in the month.

1. Navigate to `sys_properties.list`. 
2. Open the `glide.schedules.fifth` property.
3. Verify that the **Value** is set to **last**.
4. Navigate to **System Scheduler > Schedules > Schedules**, define a new schedule, and click **Submit**.
5. Open the new schedule and in the **Schedule Entries** related list, create a new entry with the following parameters:
   - When: November 29, 2012 at 10:00 to November 29, 2012 at 11:00
   - Repeats: Monthly
   - Monthly type: Day of the Week
   - Starting: November 29

   **Note:** November 29 is the Fifth Thursday in the month.

6. Click **Submit**.
7. Open the same schedule entry.

   **Note:** The message **Every month on the Fifth Thu** appears on the form.

   The schedule for the first three months is computed as:
   - November 29, 2012 (Fifth Thursday of the month)
   - December 27, 2012 (Last Thursday of the month)
   - January 31, 2013 (Fifth Thursday of the month)
8. If you set the **Value** on the **glide.schedules.fifth** property to **next** instead of **last** in step 3, the schedule for the first three months is computed as:
   - November 29, 2012 (Fifth Thursday of the month)
   - January 3, 2012 (First Thursday of the next month since December 2012 does not have five Thursdays)
   - January 31, 2013 (Fifth Thursday of the month)

9. If the **Value** on the **glide.schedules.fifth** property is set to **strict** instead of **last** in step 3, the schedule for the first three months is computed as:
   - November 29, 2012 (Fifth Thursday of the month)
   - No meeting (December 2012 skipped because it does not have five Thursdays)
   - January 31, 2013 (Fifth Thursday of the month)

### Repeat a monthly schedule

Repeat a monthly schedule to reduce the amount of time required to define schedules and to provide consistency in scheduling.

You can specify the following options for monthly schedules that start on a particular day of the month (**Monthly type** is set to **Day of the month**). The following methods are available to compute what day of the week a monthly schedule repeats on:

- **Day**: Calculates the day of the week to repeat on by determining the order of the selected starting date within the month. For example, if you specified that the starting date appears on the first Monday in the month, the schedule repeats every first Monday of every month.
- **Week**: Calculates the day of the month to repeat on by determining what week number the selected starting date appears in the month. For example, if the starting date is a Monday during the second week of the month, the schedule repeats the second Monday of every month.

Use the system property **glide.schedules.repeat_nth** to determine what method your instance uses to compute what day a repeating monthly schedule occurs on. By default, instances use the more accurate **Day** method.

**Note:** Use the **Week** method to maintain backwards compatibility with customized schedule logic. To learn more about calculations for the starting day of each month, for monthly schedules that start on the fifth instance of a day, see Fifth Instance of a Day of the Week.

The following example illustrates computing what day of the week a monthly schedule repeats on.

1. Navigate to **sys_properties.list**.
2. Open the **glide.schedules.repeat_nth** property.
3. Verify that the **Value** is set to **day**.
4. Navigate to **System Scheduler > Schedules > Schedules**, define a new schedule, and click **Submit**.
5. Open the new schedule and in the **Schedule Entries** related list, create a new entry with the following parameters:
   - When: November 5, 2012 at 10:00 to November 5, 2012 at 11:00
   - Repeats: Monthly
   - Monthly type: Day of the Week
   - Starting: November 5

   **Note:** November 5 is the first Monday in the month, but it is in the second week.

6. Click **Submit**.

7. Open **Schedule Entry**.

   **Note:** The message *Every month on the first Mon* appears on the form. The first few dates this schedule runs on are:
   - November 5, 2012 (First Monday of the month)
   - December 3, 2012 (First Monday of the month)
   - January 7, 2012 (First Monday of the month)

8. If you set the **Value** on the `glide.schedules.repeat_nth` property to **week** instead of **day** in step 3, the first few dates this schedule run on are:
   - November 5, 2012 (Schedule starts on Monday in the second week of the month)
   - December 10, 2012 (Second Monday in the month)
   - January 14, 2012 (Second Monday in the month)

**Using schedules and calendars**

Specific applications within the Now Platform generate graphical calendar displays based on schedule pages. These schedule pages appear in daily, weekly, or monthly views. Currently, the applications using schedule pages include:
- Project Management
- Maintenance Schedules
- Group On-Call Rotation
- Field Service Management

Schedule pages are records that contain the scripts that determine the functionality of the graphical display.
Because of the heavy degree of scripting involved in a schedule page, you should, for most instances, use the default schedule pages in the base platform.

The schedule page uses a URL with a series of parameters attached to generate the graphical display.

A schedule page controls calendar content (cmn_schedule_page) record.

To access Schedule Pages, navigate to **System Scheduler > Schedules > Schedule Pages**. The Schedule Pages form provides the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Field Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>String</td>
<td>General name used to identity the current schedule page.</td>
</tr>
</tbody>
</table>
| Schedule type  | String     | Schedule type is a string that is used to uniquely identify the schedule page via the "sysparm_page_schedule_type" URI parameter. For example, a schedule page could be accessed as follows:  
/show_schedule_page.do?sysparm_page_schedule_type=gantt_chart&sysparm_timeline_task_id=d530bf907f0000015ce594fd929cf6a4  
Alternatively, you can access the schedule page can by setting the "sysparm_page_sys_id" URI parameter to the unique 32 character hexadecimal system identifier of the schedule page. |
| View Type      | Choice     | Each view type displays different field combinations. There are two options available:  
• Calendars  
• Timelines |
| Description    | String     | General description that provides additional information about the current schedule page. This field is not necessary. |
| Init function name | String | The init function name specifies the name of the JavaScript function to call inside the Client script function for calendar type schedule pages. |
## Field Type Reference

<table>
<thead>
<tr>
<th>Field</th>
<th>Field Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTML</td>
<td>String</td>
<td>Jelly parses the HTML field, which is a scriptable section. It then injects it into the display page prior to the rest of the calendar. It can be used to pass in variables from the server and define extra fields are necessary.</td>
</tr>
<tr>
<td>Client script</td>
<td>String</td>
<td>The client script is a scriptable section that allows for configuring options of the schedule page display. The API is different depending on the schedule page view type.</td>
</tr>
<tr>
<td>Server AJAX processor</td>
<td>String</td>
<td>The Server AJAX processor is specific to calendar type schedule pages that is used to return a set of schedule items and spans that display.</td>
</tr>
</tbody>
</table>

### Invoke the Schedule page and view a calendar

You can use the URL from arguments module, a field decoration (dictionary attribute `ref_contributions`), or a UI Action linking to `show_schedule.doto` to invoke the Schedule page.

For example, the On-call calendar module generates the calendar from the following URL:

```
$ocf.do?
sysparm_start_date=2016-03-01&sysparm_current_view=monthly&sysparm_include_view=monthly,daily
```

This URL takes the user to the monthly calendar view dated March 1, 2016.

- The URL component `sysparm_current_view = monthly || weekly || daily` determines the current calendar view. If `sysparm_current_view` is given an invalid or empty value, it defaults to monthly view and rewrite the URL to that view. Valid values are monthly or weekly or daily.
- The URL component `sysparm_include_view = monthly,weekly,daily` determines which calendar views are available. If `sysparm_include_view` is given invalid or empty values, only the valid views appear. If all values are invalid, the default three views appears and rewrites the URL to those views. Valid values are monthly, weekly, and daily.

**Note:** The `sysparm_include_view` is only available for the new on-call calendar view.

- The URL component `sysparm_group_id=group_sys_id` determines the specified group to filter on. If `sysparm_group_id` is specified, it filters by the specified group. Valid value is a group sysId.
- The URL component `sysparm_start_date=2016-03-02` determines the date based on which every view appears. If `sysparm_start_date` is specified, it opens the calendar contesting that particular date in which
every view is selected. The format is YYYY-MM-DD. If an invalid format or date is specified, it uses the current date and rewrites the URL to that date.

Note: The `sysparm_zoom` URL component has been replaced with `sysparm_current_view` in OnCallRotation only.

Schedule calendar

Graphically represent a defined schedule and its related schedule spans.

The schedule calendar is available in day, week, or month views in calendar and timeline views.

To view the schedule calendar, click **Show Schedule** under related links in the Schedule form.

The and the icon at the upper left of the window helps you to navigate between the calendar view and the timeline view of schedules. By default, schedule appears in the **Month** view and the current day is highlighted. The calendar also provides **Day** and **Week** views. If you want to view the schedule and schedule spans of any specific day, week, or month, click and select the specific date. You can also combine the available functionalities to change the view of the calendar. For example, you can click to choose timeline view, select a particular date from
and select the **Day, Week, or Month** view.

If you want to view events for the current day, week or month, click **Today**. The left and the right arrow next to **Today** helps you to navigate to the previous or the next day, week, or month depending on the view type.

To add an event, double-click the time slot where you want to add the event. In the Add Event window, enter the required information. If you want to view the details of an event, click the event. A pop-up window appears with the details of the event.

**Event details**

To modify the start and end time for an existing non-recurring or recurring event:

- Click the event and in the Event pop-up window.
- Click **Edit** to modify the required fields.

<table>
<thead>
<tr>
<th>Modify event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the event.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of event. For example, time off, appointment, meeting.</td>
</tr>
<tr>
<td>Show as</td>
<td>Status that is visible when the event starts.</td>
</tr>
<tr>
<td>When</td>
<td>Date and time when the event starts and ends.</td>
</tr>
<tr>
<td>All day</td>
<td>Check box that indicates that the event becomes a continuous event, irrespective of the date and time specified in the When field.</td>
</tr>
<tr>
<td>Repeats</td>
<td>Value when the event must be repeated.</td>
</tr>
<tr>
<td>Repeat until</td>
<td>Date until when the event is repeated.</td>
</tr>
</tbody>
</table>

Click **Update** if you want the event to be modified with the new value.

Click **Deactivate** if you want to delete the event from that specific day until the specified end day of the event.

Click **Delete** if you want to delete the event from the day the event had started.

You can also drag a specific event to the new date or time.
• When you drag a non-recurring event, a pop-up window appears to confirm whether you want to save the event change.
• When you drag a recurring event to a new date or time, a pop-up window appears. Use it to confirm whether you want to edit all occurrences, or only the current occurrence of the event. You can choose your option, as appropriate.

Schedule calendar also provides keyboard shortcuts to help you navigate quickly. The list of navigation shortcuts appear when you click

**Domain support and schedules**

Domain separation is supported in schedules. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can control several aspects of this separation, including which users can see and access data. Activate the Domain Support [com.glide.domain] plugin to enable the domain separation functionality for schedules.

**Support level: Basic**

• Business logic: Ensure that data goes into the proper domain for the application’s service provider use cases.
• The application supports domain separation at run time. The domain separation includes separation from the user interface, cache keys, reporting, rollups, and aggregations.
• The owner of the instance must set up the application to function across multiple tenants.

Use case: When a service provider (SP) uses chat to respond to a tenant-customer’s message, the client must be able to see the SP's response.

To learn more, see Application support for domain separation.

**Overview**

The records in the Schedule [cmn_schedule], Schedule Page [cmn_schedule_page], and Timeline Page [cmn_timeline_page] tables have a defined domain.

• The child tables use the domain_master attribute to derive the domain from the parent table.
• You can find the domain_master attribute on the dictionary record for the respective table.

The following diagram illustrates the scope of domain separation in different schedule tables:
Domain support for schedules

Custom domain support implementations

Domain separation support does not automatically occur when you migrate to a new release containing a custom implementation of domain support for tables such as Schedule Entry [cmn_schedule_span]. This action avoids changing any specific configurations that you may have in place.

To implement the base system domain support for schedules, a sys.script utility is provided. To run this utility, navigate to Background > Scripts – Background. The script is listed under the com.glide.schedules plugin as fix_schedule_domain_support.js.

- The utility attempts to add the Domain [sys_domain] column to the Schedule [cmn_schedule], Schedule Page [cmn_schedule_page], and Timeline page [cmn_timeline_page] tables.
- It then attempts to add the domain_master attribute to the Schedule Entry [cmn_schedule_span], Other Schedule [cmn_other_schedule], Timeline Sub Item [cmn_timeline_sub_item], and Timeline Page Span Style [cmn_timeline_page_style] tables.
- If the script finds existing records between a child and parent record that have differing domain, the script does not introduce the domain_master attribute to the child table.

For example, consider the relationship of the Schedule [cmn_schedule] (parent) and Schedule Entry [cmn_schedule_span] (child) tables. If the Domain [sys_domain] column is available on both tables in the upgrading instance, the utility must migrate to the base system implementation of domain support for schedules.

- If the script detects records where the child Schedule Entry [cmn_schedule_span] domain differs from its parent Schedule [cmn_schedule] domain, it stops executing and logs a warning message.
- If the script does not find differing records, it deactivates and limits read access to the Domain [sys_domain] and Domain Path [sys_domain_path] columns on the Schedule Entry [cmn_schedule_span] table.
- Finally, the script adds the domain_master=schedule attribute to the dictionary file for the Schedule Entry [cmn_schedule_span] table.

Note: The domain_master attribute ensures that the child and parent record domains remain the same as the domain for the child that is derived from the specified reference field.
System scheduler

The System Scheduler application contains two separate engines for scheduling: the Scheduled Jobs engine and the Schedules engine.

System scheduler

Scheduled jobs

Scheduled Jobs executes any work that must be performed at a specific time, or on a recurring basis. The Scheduled Jobs module links to the Schedule [sys_trigger] table. Manipulating records on the Schedule table is not recommended. Use this table to view existing base system scheduled jobs.

The Scheduled Jobs module in System Definition is an admin-friendly interface for scheduling work. Use this module to create new scheduled jobs. For more information, see Create a Scheduled Job.

Schedules

Schedules are rules that include or exclude time on a calendar. They are used by service levels, inactivity monitor, and group on-call rotation. For instance, you can define a schedule to restrict service levels to only apply to weekdays during business hours. You can also exclude holidays from an on-call rotation.

For more information, see Use Schedules.

Scheduled jobs

Scheduled Jobs are automated pieces of work that can be performed at a specific time or on a recurring schedule.

You can automate the following kinds of tasks:

- Automatically generate and distribute a report
- Automatically generate and schedule an entity of records, such as an incident, change item, configuration item, from a template
- Run scheduled jobs from scripts or business rules
- Scheduling at the end of the month
- Scheduling for weekdays

For developer training, see Scheduled Script Executions and Events Objectives on the ServiceNow Developer Site.
Scheduled job states

A scheduled job can be in any one of the following states.

**Ready**
Job is ready to run at the next scheduled interval.

**Running**
Job is in the process of carrying out a task.

**Queued**
Job has been added to the scheduler queue and is waiting to run.

**Error**
Error occurred while running the job.

Create a scheduled job

Create a scheduled job on the Schedule Job [sysauto] table.

Create all new scheduled jobs using this method.

1. Navigate to **System Definition > Scheduled Jobs**.
2. Click **New**.
3. Select the appropriate type of scheduled job.

The fields presented depend on the type of scheduled job required.
Automate generation and distribution of a report
Generate and distribute scheduled reports via email.

Roles required: admin or schedule_admin

Data may not appear on reports created by an individual whose user account is deactivated. To ensure that the desired data appears, an active user must recreate the scheduled report.

1. Navigate to **System Definition > Scheduled Jobs**.
2. Click **New**.
3. Select **Automate the generation and distribution of a report**.
4. Populate the following fields:

   **Schedule a report**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name that identifies this scheduled job.</td>
</tr>
<tr>
<td>Report</td>
<td>Reference to the report you are scheduling.</td>
</tr>
<tr>
<td>Note:</td>
<td>Automatic email support is not available for Calendar, Map, and Single Score reports.</td>
</tr>
<tr>
<td>Users</td>
<td>Names of the users to send the report to at the scheduled date and time. Users must have Notification set to Enabled on their user records to receive reports.</td>
</tr>
<tr>
<td>Groups</td>
<td>Names of the groups to send the report to at the scheduled date and time.</td>
</tr>
<tr>
<td>Email addresses</td>
<td>Other email addresses to send the report to, separated by commas. If a matching user record for that address is flagged as Do not notify, this flag is respected. The user does not receive the report.</td>
</tr>
<tr>
<td>Application</td>
<td>Name of the application that contains the report. Global appears if the report is in the global scope.</td>
</tr>
<tr>
<td>Active</td>
<td>Option that indicates that scheduled job is active and should be executed at the specified date and time.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Run</td>
<td>Time interval to use for running the scheduled job:</td>
</tr>
<tr>
<td></td>
<td>• Daily: Runs daily, at a designated time.</td>
</tr>
<tr>
<td></td>
<td>• Weekly: Runs on a weekly basis, at a designated time and day of the week.</td>
</tr>
<tr>
<td></td>
<td>• Monthly: Runs on a monthly basis, at a designated time and day of the month.</td>
</tr>
<tr>
<td></td>
<td>• Periodically: Runs on a designated repeating interval.</td>
</tr>
<tr>
<td></td>
<td>• Once: Runs for a single occurrence only.</td>
</tr>
<tr>
<td></td>
<td>• On Demand: Runs immediately on demand.</td>
</tr>
<tr>
<td></td>
<td>• Business Calendar: Entry Start: Runs on the starting entry dates for the business calendar you select in the Business Calendar field. A scheduled job runs for the starting date of each of the business entries you defined for the business calendar.</td>
</tr>
<tr>
<td></td>
<td>For example, if the business calendar represents a fiscal year, and the starting date of each entry is a fiscal month, the scheduled job runs on the first day of each month.</td>
</tr>
<tr>
<td></td>
<td>• Business Calendar: Entry End: Runs for the ending date for the business calendar you select in the Business Calendar field. This selection runs in the same manner as Business Calendar: Entry Start, but for end dates of associated business calendar entries.</td>
</tr>
</tbody>
</table>

**Note:** When you select Business Calendar: Entry Start or Business Calendar: Entry End, you can apply an offset factor to schedule the job to run before or after the time span of the selected business calendar. To learn more, see the Offset type and Offset fields.

To learn more about creating and using business calendars and defining business calendar entries, see Creating business calendars and Define business calendar entries.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time zone</td>
<td>Time zone to use with the <strong>Time</strong> field entry when you specify the time at which the scheduled job run. Select a time zone entry:</td>
</tr>
<tr>
<td></td>
<td>• <strong>-None-</strong>: Use the default time zone for the logged in user who is creating the scheduled job.</td>
</tr>
<tr>
<td></td>
<td>For example, the scheduled job runs at 04:45 p.m. US/Pacific time if it is the user’s assigned time zone, and you enter 16:45 into the <strong>Time</strong> field.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Use System Time Zone</strong>: Use the default system time zone specified for the instance in which it runs.</td>
</tr>
<tr>
<td></td>
<td>For example, the scheduled job runs at 10:15 p.m. London time if Europe/London is the default system time zone for the instance, and you enter 22:15 into the <strong>Time</strong> field.</td>
</tr>
<tr>
<td></td>
<td>• Actual time zone.</td>
</tr>
<tr>
<td></td>
<td>For example, the scheduled job runs at 1:30 p.m. in the US Eastern time zone if you select <strong>US/Eastern</strong>, and enter 13:30 into the <strong>Time</strong> field.</td>
</tr>
<tr>
<td>Time</td>
<td>Time of day at which the scheduled job should run, expressed in hours, minutes, and seconds on a 24-hour clock. The selection you make in the <strong>Time zone</strong> field determines the time zone for this entry.</td>
</tr>
<tr>
<td>Day</td>
<td>Day on which the scheduled job should run.</td>
</tr>
<tr>
<td></td>
<td>• If <strong>Run</strong> is set to <strong>Weekly</strong>, select the day of the week. For example, select Wednesday.</td>
</tr>
<tr>
<td></td>
<td>• If <strong>Run</strong> is set to <strong>Monthly</strong>, select the day of the month. For example, select 25 for the 25th day of the month.</td>
</tr>
<tr>
<td></td>
<td>This field only appears if you select <strong>Monthly</strong> or <strong>Weekly</strong> in the <strong>Run</strong> field.</td>
</tr>
<tr>
<td>Repeat Interval</td>
<td>Duration of the repeat interval for each scheduled job execution. Enter the duration in the number of days, hours, or minutes. For example:</td>
</tr>
<tr>
<td></td>
<td>• To run the scheduled job every four days, enter 04 into the <strong>Days</strong> field.</td>
</tr>
<tr>
<td></td>
<td>• To run it every 26 hours, enter 26 into the <strong>Hours</strong> field.</td>
</tr>
<tr>
<td></td>
<td>• If it should repeat at an interval of 13:30:25, enter 13 into the <strong>Hours</strong> field, then 30 and 25 into the two unlabeled fields after it.</td>
</tr>
<tr>
<td>Starting</td>
<td>Date and time of the first scheduled job generation. Select the calendar date and time. This field only appears if you select <strong>Periodically</strong> in the <strong>Run</strong> field.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Business Calendar</td>
<td>Business calendar entry you are using to determine the business calendar start or end date for the scheduled job. This field appears only if you select Business Entry: Start Date or Business Entry: End Date in the Time field.</td>
</tr>
<tr>
<td>Offset type</td>
<td>Type of time offset, if any, to apply to the business calendar you selected for scheduling this job.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Past</strong>: Apply an offset factor to schedule the job to run before the start of the time span of the selected business calendar.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Future</strong>: Apply an offset factor to schedule the job to run after the end of the time span of the selected business calendar.</td>
</tr>
<tr>
<td></td>
<td>• <strong>--None--</strong>: Do not apply a time offset when scheduling this job.</td>
</tr>
<tr>
<td>Offset</td>
<td>Amount of time offset, expressed in days, hours, minutes, and seconds, to apply to the business calendar you selected for scheduling this job. For example, if you want to schedule the job to start three days, 14 hours, 10 minutes, and 45 seconds before the business calendar start date:</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Past</strong> in the Offset type field.</td>
</tr>
<tr>
<td></td>
<td>• Enter 3 into the Days field.</td>
</tr>
<tr>
<td></td>
<td>• Enter 14, 10, and 45 into the Hours field.</td>
</tr>
<tr>
<td>Priority</td>
<td>Numerical priority for the scheduled job.</td>
</tr>
<tr>
<td></td>
<td>• Set essential jobs to a priority value below 100.</td>
</tr>
<tr>
<td></td>
<td>• Set nonessential jobs to a priority above 100.</td>
</tr>
<tr>
<td></td>
<td>• If 70% or more of all scheduled jobs are <strong>Overdue</strong>, any jobs marked with a value above 100 do not run.</td>
</tr>
<tr>
<td>Conditional</td>
<td>Option for enabling the running of the scheduled job if certain conditions are met in the associated script.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Omit if no records</td>
<td>Check box that designates that generation of a scheduled job should not occur when there are no records to generate it for.</td>
</tr>
<tr>
<td>Condition</td>
<td>Conditional script that determines if a scheduled job should run. The last expression of the script should evaluate to a Boolean (true/false) value. This text box appears only if you select <strong>Conditional</strong>.</td>
</tr>
<tr>
<td>Subject</td>
<td>Subject line for the email.</td>
</tr>
<tr>
<td>Introductory Message</td>
<td>Body of the email.</td>
</tr>
<tr>
<td>Type</td>
<td>File type for the attached report. Choices are:</td>
</tr>
<tr>
<td></td>
<td>• PDF-landscape</td>
</tr>
<tr>
<td></td>
<td>• PDF</td>
</tr>
<tr>
<td></td>
<td>• Excel</td>
</tr>
<tr>
<td></td>
<td>• CSV</td>
</tr>
<tr>
<td></td>
<td>• PNG</td>
</tr>
<tr>
<td>Zip Output</td>
<td>Select to compress the scheduled report to a .zip file.</td>
</tr>
<tr>
<td>Include with</td>
<td>Click the magnifier icon to choose another active scheduled report to include with this scheduled report.</td>
</tr>
</tbody>
</table>

**Note:** An alternative for scheduling calendar and pivot table reports for email distribution is using the Publish option.

- This option creates a URL for the report, and the address appears above the report form.
- You can create an email notification with this URL and send the link to people who must see the report.
- You can also send the URL for the calendar report to a distribution list.

**Automatically generate something from a template**

Schedule the generation of entities, which include changes, incidents, and CIs.

Roles required: admin or schedule_admin

1. Navigate to **System Definition > Scheduled Jobs**.
2. Click **New**.
3. Select **Automatically generate something (a change, an incident, a CI, etc) from a template**.
4. Populate the following fields:

**Schedule entity generation**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name that identifies this scheduled job.</td>
</tr>
<tr>
<td>Active</td>
<td>Option that indicates that scheduled job is active and should be executed at the specified date and time.</td>
</tr>
<tr>
<td>Application</td>
<td>Name of the application that contains the entity. <strong>Global</strong> appears if the entity is in the global scope.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Conditional</td>
<td>Option for enabling the running of the scheduled job if certain conditions are met in the associated script.</td>
</tr>
<tr>
<td>Condition</td>
<td>Conditional script that determines if a scheduled job should run. The last expression of the script should evaluate to a Boolean (true/false) value. This text box appears only if you select <strong>Conditional</strong>.</td>
</tr>
<tr>
<td>Run</td>
<td>Time interval to use for running the scheduled job:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Daily</strong>: Runs daily, at a designated time.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Weekly</strong>: Runs on a weekly basis, at a designated time and day of the week.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Monthly</strong>: Runs on a monthly basis, at a designated time and day of the month.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Periodically</strong>: Runs on a designated repeating interval.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Once</strong>: Runs for a single occurrence only.</td>
</tr>
<tr>
<td></td>
<td>• <strong>On Demand</strong>: Runs immediately on demand.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Business Calendar: Entry Start</strong>: Runs on the starting entry dates for the business calendar you select in the <strong>Business Calendar</strong> field. A scheduled job runs for the starting date of each of the business entries you defined for the business calendar. For example, if the business calendar represents a fiscal year, and the starting date of each entry is a fiscal month, the scheduled job runs on the first day of each month.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Business Calendar: Entry End</strong>: Runs for the ending date for the business calendar you select in the <strong>Business Calendar</strong> field. This selection runs in the same manner as <strong>Business Calendar: Entry Start</strong>, but for end dates of associated business calendar entries.</td>
</tr>
<tr>
<td>Time</td>
<td>Time of day at which the scheduled job should run, expressed in hours, minutes, and seconds on a 24-hour clock. The selection you make in the <strong>Time zone</strong> field determines the time zone for this entry.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Time zone           | Time zone to use with the **Time** field entry when you specify the time at which the scheduled job run. Select a time zone entry:  
  • **-None-**: Use the default time zone for the logged in user who is creating the scheduled job.  
    For example, the scheduled job runs at 04:45 p.m. US/Pacific time if it is the user's assigned time zone, and you enter **16 : 45** into the **Time** field.  
  • **Use System Time Zone**: Use the default system time zone specified for the instance in which it runs.  
    For example, the scheduled job runs at 10:15 p.m. London time if Europe/London is the default system time zone for the instance, and you enter **22 : 15** into the **Time** field.  
  • **Actual time zone.**  
    For example, the scheduled job runs at 1:30 p.m. in the US Eastern time zone if you select **US/Eastern**, and enter **13 : 30** into the **Time** field. |
| Day                 | Day on which the scheduled job should run.  
  • If **Run** is set to **Weekly**, select the day of the week. For example, select Wednesday.  
  • If **Run** is set to **Monthly**, select the day of the month. For example, select 25 for the 25th day of the month.  
  This field only appears if you select **Monthly** or **Weekly** in the **Run** field. |
| Repeat Interval     | Duration of the repeat interval for each scheduled job execution. Enter the duration in the number of days, hours, or minutes. For example:  
  • To run the scheduled job every four days, enter **04** into the **Days** field.  
  • To run it every 26 hours, enter **26** into the **Hours** field.  
  • If it should repeat at an interval of 13:30:25, enter **13** into the **Hours** field, then **30** and **25** into the two unlabeled fields after it. |
<p>| Starting            | Date and time of the first scheduled job generation. Select the calendar date and time. This field only appears if you select <strong>Periodically</strong> in the <strong>Run</strong> field. |
| Business Calendar   | Business calendar entry you are using to determine the business calendar start or end date for the scheduled job. This field appears only if you select <strong>Business Entry: Start Date</strong> or <strong>Business Entry: End Date</strong> in the <strong>Time</strong> field. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offset type</td>
<td>Type of time offset, if any, to apply to the business calendar you selected for scheduling this job.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Past</strong>: Apply an offset factor to schedule the job to run before the start of the time span of the selected business calendar.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Future</strong>: Apply an offset factor to schedule the job to run after the end of the time span of the selected business calendar.</td>
</tr>
<tr>
<td></td>
<td>• <strong>--None--</strong>: Do not apply a time offset when scheduling this job.</td>
</tr>
<tr>
<td></td>
<td>Adding an offset factor enables scheduling of the job to run before, or after, the formal time span defined in the business calendar for the following use cases:</td>
</tr>
<tr>
<td></td>
<td>• Schedule a job at a certain time, outside of the time span for the selected business calendar.</td>
</tr>
<tr>
<td></td>
<td>• Arrange multiple jobs to run in sequence, around the time span of the selected business calendar.</td>
</tr>
<tr>
<td>Offset</td>
<td>Amount of time offset, expressed in days, hours, minutes, and seconds, to apply to the business calendar you selected for scheduling this job. For example, if you want to schedule the job to start three days, 14 hours, 10 minutes, and 45 seconds before the business calendar start date:</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Past</strong> in the <strong>Offset type</strong> field.</td>
</tr>
<tr>
<td></td>
<td>• Enter 3 into the <strong>Days</strong> field.</td>
</tr>
<tr>
<td></td>
<td>• Enter 14, 10, and 45 into the <strong>Hours</strong> field.</td>
</tr>
<tr>
<td>Generate this</td>
<td>Reference to the template record from which you are generating a scheduled job.</td>
</tr>
</tbody>
</table>

**Automatically run a script of your choosing**

Schedule both conditional and non-conditional scripts. If Domain Separation is installed in the instance, you can also select, filter, sort, and schedule scripts based on their assigned domains.

Roles required: admin or schedule_admin

The following is an example of a conditional script. It runs the scheduled job only if there are active incidents older than 30 days.

```javascript
// Only run this Scheduled Job if there are active Incidents over 30 days old
var ga = new GlideAggregate('incident');
ga.addAggregate('COUNT');
ga.addQuery('active', 'true');
```
1. Navigate to **System Definition > Scheduled Jobs**.
2. Click **New**.
3. Select **Automatically run a script of your choosing**.
4. On the form, fill in the fields.

**Schedule script execution**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name that identifies this scheduled job.</td>
</tr>
<tr>
<td>Active</td>
<td>Option that indicates that scheduled job is active and should be executed at the specified date and time.</td>
</tr>
<tr>
<td>Application</td>
<td>Name of the application that contains the script. Global appears if the script is in the global scope.</td>
</tr>
<tr>
<td>Conditional</td>
<td>Option for enabling the running of the scheduled job if certain conditions are met in the associated script.</td>
</tr>
<tr>
<td>Condition</td>
<td>Conditional script that determines if a scheduled job should run. The last expression of the script should evaluate to a Boolean (true/false) value. This text box appears only if you select <strong>Conditional</strong>.</td>
</tr>
</tbody>
</table>
### Field: Run

Time interval to use for running the scheduled job:

- **Daily**: Runs daily, at a designated time.
- **Weekly**: Runs on a weekly basis, at a designated time and day of the week.
- **Monthly**: Runs on a monthly basis, at a designated time and day of the month.
- **Periodically**: Runs on a designated repeating interval.
- **Once**: Runs for a single occurrence only.
- **On Demand**: Runs immediately on demand.
- **Business Calendar: Entry Start**: Runs on the starting entry dates for the business calendar you select in the *Business Calendar* field. A scheduled job runs for the starting date of each of the business entries you defined for the business calendar.

For example, if the business calendar represents a fiscal year, and the starting date of each entry is a fiscal month, the scheduled job runs on the first day of each month.

- **Business Calendar: Entry End**: Runs for the ending date for the business calendar you select in the *Business Calendar* field. This selection runs in the same manner as *Business Calendar: Entry Start*, but for end dates of associated business calendar entries.

**Note:** When you select *Business Calendar: Entry Start* or *Business Calendar: Entry End*, you can apply an offset factor to schedule the job to run before or after the time span of the selected business calendar. To learn more, see the *Offset type* and *Offset* fields.

To learn more about creating and using business calendars and defining business calendar entries, see [Creating business calendars](#) and [Define business calendar entries](#).

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Run   | Time interval to use for running the scheduled job:  
  - **Daily**: Runs daily, at a designated time.  
  - **Weekly**: Runs on a weekly basis, at a designated time and day of the week.  
  - **Monthly**: Runs on a monthly basis, at a designated time and day of the month.  
  - **Periodically**: Runs on a designated repeating interval.  
  - **Once**: Runs for a single occurrence only.  
  - **On Demand**: Runs immediately on demand.  
  - **Business Calendar: Entry Start**: Runs on the starting entry dates for the business calendar you select in the *Business Calendar* field. A scheduled job runs for the starting date of each of the business entries you defined for the business calendar. For example, if the business calendar represents a fiscal year, and the starting date of each entry is a fiscal month, the scheduled job runs on the first day of each month.  
  - **Business Calendar: Entry End**: Runs for the ending date for the business calendar you select in the *Business Calendar* field. This selection runs in the same manner as *Business Calendar: Entry Start*, but for end dates of associated business calendar entries. |
| Day   | Day on which the scheduled job should run.  
  - If *Run* is set to **Weekly**, select the day of the week. For example, select Wednesday.  
  - If *Run* is set to **Monthly**, select the day of the month. For example, select 25 for the 25th day of the month.  
  
  This field only appears if you select **Monthly** or **Weekly** in the *Run* field. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Repeat Interval | Duration of the repeat interval for each scheduled job execution. Enter the duration in the number of days, hours, or minutes. For example:  
  • To run the scheduled job every four days, enter 04 into the **Days** field.  
  • To run it every 26 hours, enter 26 into the **Hours** field.  
  • If it should repeat at an interval of 13:30:25, enter 13 into the **Hours** field, then 30 and 25 into the two unlabeled fields after it.                                                                                                                                                                                                                                                                                                                                 |
| Time zone     | Time zone to use with the **Time** field entry when you specify the time at which the scheduled job run. Select a time zone entry:  
  • **-None-**: Use the default time zone for the logged in user who is creating the scheduled job.  
    For example, the scheduled job runs at 04:45 p.m. US/Pacific time if it is the user’s assigned time zone, and you enter 16:45 into the **Time** field.  
  • **Use System Time Zone**: Use the default system time zone specified for the instance in which it runs.  
    For example, the scheduled job runs at 10:15 p.m. London time if Europe/London is the default system time zone for the instance, and you enter 22:15 into the **Time** field.  
  • Actual time zone.  
    For example, the scheduled job runs at 1:30 p.m. in the US Eastern time zone if you select **US/Eastern**, and enter 13:30 into the **Time** field.                                                                                                                                                                                                                           |
| Time          | Time of day at which the scheduled job should run, expressed in hours, minutes, and seconds on a 24-hour clock. The selection you make in the **Time zone** field determines the time zone for this entry.                                                                                                                                                                                                                                                  |
| Day           | Day on which the scheduled job should run.  
  • If **Run** is set to **Weekly**, select the day of the week. For example, select Wednesday.  
  • If **Run** is set to **Monthly**, select the day of the month. For example, select 25 for the 25th day of the month.                                                                                                                                                                                                                                                                                                                |

This field only appears if you select **Monthly** or **Weekly** in the **Run** field.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repeat Interval</td>
<td>Duration of the repeat interval for each scheduled job execution. Enter the duration in the number of days, hours, or minutes. For example:</td>
</tr>
<tr>
<td></td>
<td>- To run the scheduled job every four days, enter 04 into the <strong>Days</strong> field.</td>
</tr>
<tr>
<td></td>
<td>- To run it every 26 hours, enter 26 into the <strong>Hours</strong> field.</td>
</tr>
<tr>
<td></td>
<td>- If it should repeat at an interval of 13:30:25, enter 13 into the <strong>Hours</strong> field, then 30 and 25 into the two unlabeled fields after it.</td>
</tr>
<tr>
<td>Starting</td>
<td>Date and time of the first scheduled job generation. Select the calendar date and time. This field only appears if you select <strong>Periodically</strong> in the <strong>Run</strong> field.</td>
</tr>
<tr>
<td>Business Calendar</td>
<td>Business calendar entry you are using to determine the business calendar start or end date for the scheduled job. This field appears only if you select <strong>Business Entry: Start Date</strong> or <strong>Business Entry: End Date</strong> in the <strong>Time</strong> field.</td>
</tr>
<tr>
<td>Offset type</td>
<td>Type of time offset, if any, to apply to the business calendar you selected for scheduling this job.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Past</strong>: Apply an offset factor to schedule the job to run before the start of the time span of the selected business calendar.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Future</strong>: Apply an offset factor to schedule the job to run after the end of the time span of the selected business calendar.</td>
</tr>
<tr>
<td></td>
<td>- <strong>--None--</strong>: Do not apply a time offset when scheduling this job.</td>
</tr>
</tbody>
</table>

Adding an offset factor enables scheduling of the job to run before, or after, the formal time span defined in the business calendar for the following use cases:

- Schedule a job at a certain time, outside of the time span for the selected business calendar.
- Arrange multiple jobs to run in sequence, around the time span of the selected business calendar.

The **Offset type** and **Offset** fields only appear if you select **Business Calendar: Entry Start** or **Business Calendar: Entry End** in the **Run** field.
Field | Description
---|---
Offset | Amount of time offset, expressed in days, hours, minutes, and seconds, to apply to the business calendar you selected for scheduling this job. For example, if you want to schedule the job to start three days, 14 hours, 10 minutes, and 45 seconds before the business calendar start date:
- Select Past in the Offset type field.
- Enter 3 into the Days field.
- Enter 14, 10, and 45 into the Hours field.
The Offset Days and Hours fields only appear if you select Business Calendar: Entry Start or Business Calendar: Entry End in the Run field, and Past or Future in the Offset type field.
Run as [Optional] | Select another user to run the script execution as. Configure the form to add this field if it is not present.
Run this script | Name of the script to run at the scheduled date and time. For example, copy script logic from a business rule, or call a script include.

5. If Domain Separation is installed in this instance, the following fields also appear for selecting, sorting, and scheduling jobs by domain.

**Note:** The Domain Support - Domain Extensions Installer plugin installs these fields. To learn more, see Request domain separation.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain iterator</td>
<td>Check box that enables this job to run across multiple domains. If selected, the Domain source table and Domain source filter fields appear.</td>
</tr>
<tr>
<td>Domain source table</td>
<td>Name of the domain-separated table that is the source of the domains in which the scheduled job should run. For example, select Department (cmn_department) if you want to use it as the source of the assigned domains used to schedule scripts. The scheduled job determines these domains from the sys_domain field of the source table records. To learn more, see Domain assignment.</td>
</tr>
</tbody>
</table>

**Note:** It's a good idea to create a domain-separated table solely dedicated to sourcing domains, unless you have a use case that warrants using an existing one. If you do create a new one, simply select it using this field.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain source filter</td>
<td>Optional condition you can specify to filter the records queried from the selected domain source table.</td>
</tr>
<tr>
<td></td>
<td>a. Select the field to use for filtering records.</td>
</tr>
<tr>
<td></td>
<td>b. Add filtering conditions and operators to narrow the domain selection criteria. To learn more, see Filters.</td>
</tr>
</tbody>
</table>

The following processing takes place when scheduling a job in a domain-separated instance:

- It first queries the selected domain source table.
- If you specified a condition in the **Domain source filter** field, it applies the filtering condition to narrow down the resulting set of records.
- Finally, it retrieves its list of unique domains from the sys_domain columns of these records.

6. Click **Update** to update the scheduled job, **Execute Now** to execute the scheduled script immediately, or **Delete** to delete the job.

**Special cases in job schedules**

Some special cases require care in job scheduling.

**End of the month schedules**

Because months have different lengths, take care when scheduling jobs for the end of the month.

- Scheduling an event for the 29th or 30th is not recommended, because the scheduled job is executed in months (like February) which are shorter than those dates.
- If an event is scheduled for the 31st, it executes on the last day of the month, even if the month is shorter.

For example, something scheduled to run on the 31st of the month runs on February 28 or February 29 in a leap year.

**Weekday schedules**

For scheduled scripts, use the following script to run only on weekdays:

```javascript
(function isWeekday() {
    var gDate = new GlideDate(); //Uses your Timezone!
    var day = gDate.getByFormat('EEEE'); //Gets name of day
    switch(day) {
        case "Saturday":
        case "Sunday":
            isWeekday = false;
            break;
        default:
            isWeekday = true;
    }
    return isWeekday;
})();
```
Scheduled jobs from scripts

To execute a scheduled job triggered by an event, use the following script:

```javascript
//Execute a scheduled script job
var rec = new GlideRecord('sysauto_script');
rec.get('name', 'YOUR_JOB_NAME_HERE');
SncTriggerSynchronizer.executeNow(rec);
```

You can run the script using one of several tables:
- scheduled_import_set (Scheduled Import Sets)
- sysauto_script (Scheduled Script Execution)
- sysauto_template (Scheduled Template Generation)
- sysauto_report (Scheduled Report)

**Note:** `SncTriggerSynchronizer` does not provide methods to execute scheduled jobs in the future.

Running schedule jobs imported from another instance

To prevent unexpected data changes, Schedule Item [sys_trigger] records are not created for Scheduled Jobs [sysauto] imported from an XML file such as an update set. To run a scheduled job imported from another instance, update the scheduled job record.

View a schedule item

You can view scheduled items, which are individual instances of a scheduled job, from the system scheduler.

Navigate to System Scheduler > Today's Scheduled Jobs.

**Note:** It is inadvisable to modify the schedule items themselves. It is best to modify the scheduled jobs that contain them.

Each schedule item appears on the table listing.

Event scheduling

You can use various tools for scheduling actions or tasks to happen in the future.

**Maintenance schedules**

Changes to the CMDB can be managed through the Maintenance Schedules plugin, which enables changes to be proposed and viewed through a timeline.

**On-call rotation**

The Group On-Call Rotation plugin enables a schedule to be defined to determine what users are primary contacts during particular hours of the day.

**Scheduled reports**

Once you define reports, you can schedule them for emailing at a specific time, or at regular intervals, using the reporting interface.

**Scheduled workflows**
Workflows provide a robust system for automating advanced multi-step processes. Workflows are triggered by conditions, like business rules, or they can be scheduled for a particular time/recurring schedule, like scheduled jobs.

**Scheduled jobs**

Scheduled jobs are scripts you can specify should automatically generate at a specific date and time, or on a repeating basis.

**Event registry**

You can use events to schedule actions or tasks to occur when conditions are fulfilled.

For example:

- **kb.view**
  An event triggered when a user views a Knowledge Base article. You use it to trigger the script action Knowledge View that create a Knowledge Use record every time an article is viewed.

- **incident.commented**
  An event triggered when a user comments on an article, used by two incidents commented email notifications.

**Inactivity Monitors**

If a record has not been updated for a defined length of time, an inactivity monitor triggers an event.

**Script Actions**

Scripts that trigger when an event is recorded in the log. You can set scripts to execute whenever a particular activity occurs in the platform, rather than at a particular time, such as scheduled jobs, or in response to particular conditions, such as Business rules.

**Notifications**

You can also use events to trigger Email Notifications when an event is recorded in the log.

**Register an event**

You can register an event for a specific table and a business rule that fires the event.

1. To register an event, browse to **System Policy > Events > Registry**, and then click **New**.
2. On the form fill in the fields.

**Event Registration Form Completion**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of your new event.</td>
</tr>
<tr>
<td>Table</td>
<td>Database table for this event.</td>
</tr>
<tr>
<td>Description</td>
<td>Short description of the purpose of the event.</td>
</tr>
<tr>
<td>Fired by</td>
<td>Name of the business rule that runs the event.</td>
</tr>
</tbody>
</table>

Note: Only tables and database views that are in the same scope as the event appear on the listing.
### Set an inactivity monitor

You can set an inactivity monitor that triggers an event for a task record when the task has been inactive for a certain amount of time.

If the task remains inactive, the monitor repeats at regular intervals. User updates to the task record restart the monitor. If reset conditions you defined for it have not been met, the monitor does not restart when you update the task record. Inactivity monitors only apply to records on tables that extend the `Task` table, or the `Task` table itself.

When an inactivity monitor triggers, it generates an event in the form `<tablename>.inactivity` (for example, `incident.inactivity`). Define an email notification or script action to drive further action for the inactivity monitor.

A record's activity is only based on user updates. System updates do not count as activity.

1. Navigate to **System Policy > SLA > Inactivity Monitors** and click **New**.
2. Give the inactivity monitor a name.
3. Specify the type of record to monitor in the **Table** field.
4. Specify how long the inactivity monitor should wait before sending each notification in the **Wait** field.
5. Specify any additional conditions in the **Condition** field.

   At least one condition must be specified for the inactivity monitor to work.
   - If you are using incident auto-close, add a Reset condition because, if you don't, auto-close won't work properly. To prevent this reset, set a **Reset Condition** on your inactivity monitor. To learn more about Incident auto-close, see [Configure incidents to close automatically](#).
   - All conditions need to be True per user update for the Inactivity Monitor to start running. For example, Set this condition only works if the due date is earlier than the current date when user updates the task.

6. Specify an **Order** if multiple inactivity monitors might have their conditions met for a given record - the one with the lowest order is used.
7. Click **Save**.

**Note:** If you change conditions on an inactivity monitor, the monitor stops tracking previously tracked records. It does not track records that you created before the inactivity monitor, even if the record meets all other conditions.

### Escalation intervals and pause conditions

Escalation Intervals and Pause Conditions are not relevant to an inactivity monitor.

The related list and field are available because the inactivity monitor table extends the table used for SLAs, but these elements are not used in any way when an inactivity monitor attaches or is triggered.
Viewing record information over time

You can use three different interfaces to view record information over time: reports and performance analytics, timeline pages, schedule pages.

Reports and performance analytics

![Incidents Resolved per Month by Assignment Group (column chart)](chart)

Report example

You can visualize data in two ways:
- **Reporting** enables users to generate charts from data within the platform in various formats. Reporting is available as a standard part of the platform and offers a snapshot of current data.
- **Performance Analytics** enable you to track and aggregate data over time. For example, you can measure how many tickets are resolved each week per assignment group. Performance Analytics is enabled for the Incident table by default. To track data for other tables and applications you must license [Activating your Performance Analytics subscription](#).
Timeline pages

Timeline pages example

This type of page enables you to define linear time lines from records with time information.
Schedule pages

Timeline pages

Use timeline pages to track any activity bounded by two dates, such as change request start and end dates, or incident open and close dates. Administrators can create timeline pages, which are user interactive.

Features

- Make selected timelines available to users by role.
- Select perspective from daily to yearly views.
- Create dynamic labels for timeline spans.
- Configure tooltips for each span.
- Permit span dragging and resizing by users.
- Lock timelines to prevent editing.
Viewing timelines

By default, only administrators have a module to access timeline records. ITIL users can only view timelines by selecting a context menu item from an incident record.
Administrator role users

Users with an administrator role can view timelines from the timeline page records.

1. Navigate to System UI > Timeline Pages.
2. Select a timeline record to view.
3. Click View Timeline.

Other users

By default, timeline metrics only appear for incident records. ITIL users can view timelines associated with any task record where the metrics are set to appear as timeline records. To view the Assigned to duration and the State duration metric timelines, ITIL users can select the Metrics Timeline context menu UI action.

1. Navigate to active task record, such as an incident.
2. Right-click the banner, and select Metrics Timeline.

To enable non-administrators to view other timelines, create a custom module.

Timing functionality

Timing functionality are tools that exist to answer the question "How Long?"

Metric definitions

Defined metrics can track how long an audited field holds a certain value.

For instance, a metric can track how long an incident is assigned to an individual, or how long an incident is in the state Active.

Time configuration SLAs

Service Level Agreements time how long a task meets a certain condition, and is primarily used to ensure that tasks are handled within a pre-determined time limit.

SLAs define the following conditions:

• Start Conditions
• Pause Conditions
• Stop Conditions

Once a task meets the Start Conditions, the SLA will time how long the task remains in that condition (unless it meets Pause Conditions). The timer will end if the Stop Conditions are met. If the time-limit is passed, the SLA will be marked breached.

Notifications can be driven off of the SLA to warn interested parties as the time limit approaches.

For more information on SLA configuration, see Configure SLAs.

Time worked fields

The Task [task] table provides a time-tracking field called Time worked. This field measures how long a record has been viewed in order to measure work time on a ticket.
Any table that extends Task can use this field. To add the field, configure the form.

As the record is viewed, the timer counts upward. To pause the timer, click the stop icon ( ].

To resume the timer, click the start icon ( ].

When the task is saved, the amount of new time in the timer is used to generate a record on the Time Worked table. This table can be viewed as a related list on the task form.

By default, the time displayed in the Time worked field displays a cumulative value stored in the task record. If you modify a Time Worked record, the changes will not be reflected in the task timer.

You can set the property com.snc.time_worked.update_task_timer to enable updating of the task timer value based on changes to the time worked records. This is accomplished through the Update task timer business rule.

Create a timeline page

Create a timeline page to track any activity bounded by two dates.

Navigate to System UI > Timeline Pages and create a new record (see table for field descriptions).

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name that describes the function of this timeline. For example, High Priority Change Requests.</td>
</tr>
<tr>
<td>Table</td>
<td>Name of the table associated with this timeline, such as Change Request [change_request].</td>
</tr>
<tr>
<td>Start date field</td>
<td>Time-related field from the specified table to use as the start date for the timeline. The timeline begins with the span for the record with the earliest start date from this field, after it applies the filter and sort order. For example, you can select Updated as the start date field. It then starts the span for each active change request on the date it was updated to a high priority.</td>
</tr>
<tr>
<td>End date field</td>
<td>Time-related field from the specified table to use as the end date for the timeline. The timeline ends with the span for the record with the latest date from this field, after it applies the filter and sort order. For example, you can select Closed as the end date field and display all high priority change requests by the date on which they were closed.</td>
</tr>
</tbody>
</table>

Display Options

Show grid lines     | Select this check box to show horizontal background shading to highlight alternate spans. |
Show left pane      | Select this check box to show label text in a pane on the left of the timeline. The text that appears in this pane is defined in Span text fields. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show summary pane</td>
<td>Select this check box to show the pink, perspective slider at the bottom of the timeline. Move the slider from right to left to scroll across the chart. Adjust the end points of the slider to change the magnification. A narrow slider zooms in on the spans and provides a more detailed view. A wide slider pulls the view out and makes more of the timeline visible on the screen.</td>
</tr>
<tr>
<td>Auto refresh</td>
<td>Select an automatic refresh interval or disable automatic refresh. When auto refresh is disabled, the timeline adjusts only when the browser is manually refreshed or when a start or end date field is updated in a record.</td>
</tr>
<tr>
<td>CSS span color</td>
<td>Enter a custom span color using any CSS color format, such as RGB or hexadecimal. If this field is blank, the default span color, light blue, is used. The dark blue color indicates tasks that have a planned start date only, with no planned end date. Adding a planned end date updates the color to light blue.</td>
</tr>
<tr>
<td>Show span text</td>
<td>Select this check box to display the content of the <strong>Span text fields</strong> as labels below each span.</td>
</tr>
<tr>
<td>Span text fields</td>
<td>Select fields from the specified table to have those values appear as span labels. For example, you might select <strong>Number</strong> and <strong>Short description</strong>. The span labels also appear in the left pane if the left pane is visible.</td>
</tr>
<tr>
<td>Show tooltips</td>
<td>Select this check box to display tooltips when the cursor rests on a span.</td>
</tr>
<tr>
<td>Tooltip text fields</td>
<td>Select from the specified table the fields whose values appear as tooltips. For example, you might select <strong>Category</strong>, <strong>Assigned to</strong>, and <strong>Due date</strong>.</td>
</tr>
</tbody>
</table>

**Filtering and Sorting**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Create a condition to filter the results that appear in the timeline. For example, a condition that displays only active, high priority incidents. Add the condition count to a condition field to preview what records will be returned by this condition set.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform custom sort?</td>
<td>Select this check box to enable custom sorting. Configure the sort order by selecting fields in the <strong>Sort by</strong> and <strong>Sort by order</strong> fields.</td>
</tr>
<tr>
<td>Sort by</td>
<td>Select any field in the list for sorting the spans in the timeline. Common practice is to select either the <strong>Start date field</strong> or the <strong>End date field</strong> as the sorting field. If you select a different sorting field, also include that field in the list of <strong>Tooltip text fields</strong> to give users a way of discovering the sort criteria.</td>
</tr>
<tr>
<td>Sort by order</td>
<td>Select the sort order for the sorting fields selected.</td>
</tr>
<tr>
<td>Interactive Options</td>
<td></td>
</tr>
<tr>
<td>Allow horizontal moving?</td>
<td>Select this check box to permit users to drag timeline spans horizontally. Dragging changes the start and end dates and updates the record.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Allow start time dragging?</td>
<td>Select this check box to permit users to update the record by dragging the start time of a span.</td>
</tr>
<tr>
<td>Allow end time dragging?</td>
<td>Select this check box to permit users to update the record by dragging the end time of a span.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Range calculator</td>
<td>Specify a script include that calculates range restrictions and processes parent updates, if appropriate.</td>
</tr>
</tbody>
</table>

A completed Timeline Page record looks like this.
Customize the timeline page span style

The Timeline Page Span Styles related list allows you to define conditional span styles.

1. Navigate to **System UI > Timeline Pages**.
2. Open the timeline page for which you want to define the span style.
3. Go to the Timeline Page Span Styles related list and click **New**.
4. Fill in the form and click **Submit**.

### Customizing timeline page span styles

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition</td>
<td><strong>Condition Builder</strong> that filters the results that appear in the timeline.</td>
</tr>
<tr>
<td>Label color</td>
<td>Color for the text under each span.</td>
</tr>
<tr>
<td>Label decoration</td>
<td>Character style for the text under each span: <strong>Bold</strong>, <strong>Italic</strong>, <strong>Underline</strong>, or <strong>Line-through</strong>.</td>
</tr>
<tr>
<td>Order</td>
<td>Number to determine the sequence in which the style conditions are evaluated. Style conditions with a lower order are evaluated first.</td>
</tr>
<tr>
<td>Span color</td>
<td>Color of each span.</td>
</tr>
<tr>
<td>Timeline page</td>
<td>Timeline page to which the span style applies. By default, the span applies to the current timeline.</td>
</tr>
</tbody>
</table>

### Timeline sub item

Use the Timeline Sub Items related list to define child spans for the timeline, based on records in a table that references the parent timeline’s table.

You can create a timeline sub item generate a hierarchical relationship, starting from a timeline page to any number of levels. For example, if there is a timeline page for a release, the sub item might be sprints, and the sprint might have stories as a sub item.

1. Navigate to **System UI > Timeline Pages**.
2. Open the timeline page for which you want to add a sub item.
3. Go to the Timeline Sub Items related list and click **New**.
4. Fill in the form (see table for field descriptions) and click **Submit**.

### Timeline Sub Items

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent</td>
<td>[Read-only] Identifies the parent of the timeline sub item.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter a unique name that describes the function of this timeline. For example, Sprints for late Priority Changes.</td>
</tr>
<tr>
<td>Table</td>
<td>Select the table called by this timeline. The selected table must contain at least one field that references the table you selected for the parent timeline page. For example, if the parent timeline page uses the Scrum Release [rm_release_scrum] table, you might choose the Sprint [rm_sprint] table for a timeline sub item.</td>
</tr>
<tr>
<td>Field</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Start date field</td>
<td>Select a time-related field from the specified table to use as the start date for the timeline. For example, Planned start date.</td>
</tr>
<tr>
<td>End date field</td>
<td>Select a time-related field from the specified table to use as the end date for the timeline. For example, Planned end date.</td>
</tr>
<tr>
<td>Parent Reference Column</td>
<td>Select a reference field on which to base the timeline connection between the sub item records and the parent records.</td>
</tr>
<tr>
<td></td>
<td>• If multiple reference fields are available, choose the reference field that forms part of the hierarchy modeled by this timeline.</td>
</tr>
<tr>
<td></td>
<td>• If this list is blank, the sub item table contains no reference fields to the parent table. In this case, you must choose a different table</td>
</tr>
<tr>
<td></td>
<td>for the sub item. ServiceNow uses the parent reference column to determine which records appear at each level of the timeline.</td>
</tr>
</tbody>
</table>

**Display Options**

| CSS span color               | Enter a custom span color using any CSS color format, such as RGB or hexadecimal. If this field is blank, it uses the default span color, light blue. The dark blue color indicates tasks with a planned start date only, with no planned end date. Adding a planned end date updates the color to light blue. |
| Span text fields             | Select fields from the specified table to have those values appear as span labels. For example, you might select **Number** and **Short description**. If the timeline displays the left pane, span labels also appear in the left pane. |
| Tooltip text fields          | Select fields from the specified table to have those values appear as tooltips. For example, you might select **Category**, **Assigned to**, and **Due date**. |

**Filtering and Sorting**

| Condition builder            | Create a condition to filter the results that appear in the sub item. For example, you might create a condition that displays only active, high priority incidents. |
| Perform custom sort          | Select this check box to enable custom sorting. Configure the sort order by selecting fields in the **Sort by** and **Sort by order** fields. |
| Sort by                      | Select any field in the list for sorting the spans in the timeline. Common practice is to select either the **Start date field** or the **End date field** as the sorting field. If you select a different sorting field, also include that field in the list of tooltip text fields to give users a way of discovering the sort criteria. |
| Sort by order                | Select the sort order for the sorting fields selected.                                                                                       |

**Interactive options**
### ServiceNow

#### DocVersion

#### Now Platform administration

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow horizontal moving?</td>
<td>Select this check box to permit users to drag timeline spans horizontally. Dragging changes the start and end dates and updates the record.</td>
</tr>
<tr>
<td>Allow start time dragging?</td>
<td>Select this check box to permit users to update the record by dragging the start time of a span.</td>
</tr>
<tr>
<td>Allow end time dragging?</td>
<td>Select this check box to permit users to update the record by dragging the end time of a span.</td>
</tr>
</tbody>
</table>

**Restriction**

Specify the behavior when you drag a child span. This option is available only if you did not specify Range calculator for the parent timeline page.

- **None**: No restriction is in place.
- **Restrict by parent**: Move the child span only within the time frame defined by the parent span.
- **Update parent**: Update the span when you move the child span outside the time frame defined by the parent span.

---

**Display a metric as a timeline**

Administrators can enable users to display any metric on a timeline by activating the **Timeline Metrics** UI action.

1. Navigate to **Metrics > Definitions**.
2. Select the metric you want to display on a timeline. For example, Problem State Duration.
3. Select the **Timeline** check box.
4. **Click Update.**

The UI action is available on the same table as the metric. By default, only Incident metrics are available.

**Make a timeline visible to a selected user**

Create a custom module within an application and defining the roles that can access it, to make selected timelines available to users.

To permit these users to update task records directly from the timeline, configure the timeline to enable span dragging.

**Note:** Timelines delivered by a custom module are not entirely dynamic. The left pane, summary pane, auto-refresh feature, and the grid lines are not dynamic, and do not reflect updates to the timeline record after creating the module link. However, the data represented by the spans, labels, and tooltips display all updates in the custom module.

To create a timeline page module:

1. **Click the Edit application** icon on an application (such as Incident) in the navigation pane.
2. In the application Modules related list, click **New**.
3. **Configure the Module form to add the Timeline page field.**
4. **Fill in the form as described in the table and click Submit.**

The Module form provides the following fields.
# Making timelines visible to selected users

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Name of the module as it appears in the navigation pane. For example, you might use Planning Timeline.</td>
</tr>
<tr>
<td>Order</td>
<td>Number to determine the sequence in which this condition should be evaluated if more than one matching condition exists. Conditions with a lower order are evaluated first.</td>
</tr>
<tr>
<td>Application</td>
<td>Application for the new module.</td>
</tr>
<tr>
<td>Hint</td>
<td>Brief description of the module that appears when the user places the cursor over the module name. For example, you might enter Weekly view of high priority changes.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box that enables the module for the defined roles. Clear this check box to disable the module for all users.</td>
</tr>
<tr>
<td>Image</td>
<td>Icon that should appear with the module name.</td>
</tr>
<tr>
<td>Link type</td>
<td>Select Timeline Page. When you select this link, the Timeline Page field appears.</td>
</tr>
<tr>
<td>Timeline Page</td>
<td>Timeline page you want to appear in this module. For example, for the Change application select a change-related timeline, for the Incident application select an incident-related timeline.</td>
</tr>
<tr>
<td>Roles</td>
<td>Roles that can access this module.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Override application menu roles</td>
<td>Check box that indicates that this module should appear when the user has the specified roles. Otherwise, the user must have the roles specified by both the application menu and the module.</td>
</tr>
</tbody>
</table>

The completed module form looks like this.
A module is a link or separator in the application menu. A link gives users quick access to items like a homepage or a list of records. A separator is a horizontal line that you can use to separate modules into sections. More info

Title: Planning Timeline
Application: Global
Application menu: Incident
Hint: Weekly view of high priority changes
Order:

Visibility
Roles: Itil_admin
Override application menu roles: 
Active: 

Link Type
Select the type of link for the module or select separator to create a horizontal line. The fields below change depending on your selection.
Link type: Timeline Page
Timeline page: Change Schedule

Submit
**Range calculator scripts**

You can specify a script include that calculates range restrictions and processes parent updates in a timeline page.

**Range Calculator Scripts**

Following are three examples of script includes that help specify range restrictions.

**ExampleUpdateParentsRangeCalculator**

Updates parent records when a child record span is moved or resized in the timeline.

```javascript
var ExampleUpdateParentsRangeCalculator = Class.create();
ExampleUpdateParentsRangeCalculator.prototype = {
    initialize: function() { },
    updateParents: function(id, table, startDate, endDate){
        if (table == "rm_sprint"){
            var releaseID;
            var sprint = new GlideRecord(table);
            sprint.addQuery('sys_id', id);
            sprint.query();
            if (sprint.next())
                releaseID = sprint.release + "";
            if (releaseID) {
                var now_GR = new GlideRecord("rm_release_scrum");
                gr.addQuery("sys_id", releaseID);
                gr.query();
                if (gr.next()) {
                    if (startDate && startDate < this.getTimeMs(gr.start_date))
                        gr.start_date = this.getTimeObject(startDate);
                    if (endDate && endDate > this.getTimeMs(gr.end_date))
                        gr.end_date = this.getTimeObject(endDate);
                    gr.update();
                }
            }
        }
        },
    getMinRangeDetails: function(id, table){ return [-1, -1, "", "];
},
    getMaxRangeDetails: function(id, table){ return [-1, -1, ""];
},
    getTimeMs: function(date){
        return new GlideScheduleDateTime(date).getMS();
},
    getTimeObject: function(timeMS) {
        var gdt = new GlideDateTime();
        gdt.setNumericValue(timeMS);
        return gdt;
    },
    logMessage: function(message){ gs.log(message); },
    type: 'ExampleUpdateParentsRangeCalculator'
}
```

In this example, the span is identified based on the id and table from function(id, table, startDate, endDate).

**ExampleMinRangeCalculator**

Defines the earliest start date and the latest end date for a specified span.

```javascript
var ExampleMinRangeCalculator = Class.create();
ExampleMinRangeCalculator.prototype = {
    initialize: function() { },
    updateParents: function(id, table, startDate, endDate){
    },
    getMinRangeDetails: function(id, table){ return [-1, -1, "", ""];
},
    getMaxRangeDetails: function(id, table){ return [-1, -1, ""];
},
    getTimeMs: function(date){
        return new GlideScheduleDateTime(date).getMS();
},
    getTimeObject: function(timeMS) {
        var gdt = new GlideDateTime();
        gdt.setNumericValue(timeMS);
        return gdt;
    },
    logMessage: function(message){ gs.log(message); },
    type: 'ExampleMinRangeCalculator'
}
```

In this example, the span is identified based on the id and table from function(id, table, startDate, endDate).
var minID = "";
var maxID = "";
if (table == "rm_release_scrum"){
  var now_GR = new GlideRecord("rm_sprint");
  gr.addQuery("release", id);
  gr.query();
  while(gr.next()){
    var start = this.getTimeMs(gr["start_date"]);
    var end = this.getTimeMs(gr["end_date"]);
    var id = gr["sys_id"];
    if (min == -1 || start <= min){
      if (start != min)
        minID = "";
      min = start;
      minID +="," + id;
    }
    if (max == -1 || end >= max){
      if (end != max)
        maxID = "";
      max = end;
      maxID += "," + id;
    }
  }
}
return [min, max, minID, maxID];
}

getMaxRangeDetails: function(id, table){ return [-1, -1, "", ""]; },
getTimeMs: function(date){ return new GlideScheduleDateTime(date).getMS(); },
getTimeObject: function(timeMS) {
  var gdt = new GlideDateTime();
  gdt.setNumericValue(timeMS);
  return gdt; },
logMessage: function(message){ gs.log(message); },
type: 'ExampleUpdateParentsRangeCalculator'
}

ExampleMaxRangeCalculator

Defines the earliest start date and the latest end date for a specified span.

var ExampleMaxRangeCalculator = Class.create();
ExampleMaxRangeCalculator.prototype = {
  initialize: function() { },
  updateParents: function(id, table, startDate, endDate){ },
  getMinRangeDetails: function(id, table){ return [-1, -1, "", ""]; },
  getMaxRangeDetails: function(id, table){
    if (table == "rm_sprint"){
      var sprint = new GlideRecord(table);
      sprint.addQuery('sys_id', id);
      sprint.query();
      if (sprint.next())
        releaseID = sprint.release + "";
      if (releaseID) {
        var now_GR = new GlideRecord("rm_release_scrum");
        gr.addQuery("sys_id", releaseID);
        gr.query();
        if (gr.next())
          return [this.getTimeMs(gr.start_date),
                  this.getTimeMs(gr.end_date), gr.sys_id];
    }
  }
  return [-1, -1, ""];
Timelines

Timelines display a linear calendar of tasks, such as incidents and change requests, defined by their start and end dates.

A span represents each task on the timeline, which is displayed as a horizontal bar and may have distinctive color coding. Each span has a label and can have tooltip text containing additional information about the task. You can also change the perspective of the calendar for a more granular view of the data.

Changes in perspective

Use the range selectors at the top of the timeline to change the perspective.

The increments go from one day to one year. To limit the timeline to an increment between the start date of the first span and the end date of the last span, click Max. Use the starting and ending calendar fields to select the timeline perspective. These fields control the same perspective as the slider at the bottom of the timeline. The green, vertical line indicates the current date and time, and sweeps across the timeline automatically.

Timeline Perspective Slider

The pink slider at the bottom of the timeline offers another way to change the perspective. Move the slider from right to left to view all the spans on a long timeline. Adjust the end points of the slider to make arbitrary changes to the magnification. A narrow slider zooms in on the spans and provides a more detailed view of complex timelines. A wide slider pulls the view out and makes more of the timeline visible on the screen.
Managing spans
You can view span details, focus and zoom spans, and edit spans.

A span represents each task on the timeline, which is displayed as a horizontal bar and may have distinctive color coding. Each span has a label and can have tooltip text containing additional information about the task. You can also change the perspective of the calendar for a more granular view of the data.

Span details
If the left navigation pane is visible, the span label is visible in the left pane.
If the left pane is hidden, point the cursor over a span to view the tooltip.

Timeline Tooltip

Span focus and zoom
You can use keyboard shortcuts when using timelines.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Shortcut</th>
</tr>
</thead>
<tbody>
<tr>
<td>Macintosh</td>
<td>Command + Click</td>
</tr>
<tr>
<td>Windows</td>
<td>Control + Click</td>
</tr>
</tbody>
</table>

Span edits
If the timeline has been configured for editing (horizontal moving, start and end date dragging), use the mouse to adjust the spans to suit your needs.
Move the start or end dates to change the duration of the task.
Client transaction timings

The Client Transaction Timings plugin enhances the system logs by providing additional information about the durations of transactions taking place between the client and the server.

You can track down performance issues to their source by viewing where the time is being consumed, and how time was spent during a transaction.

This plugin requires the Response Time Indicator Response Time Indicator to be enabled, and collects information from the following browsers:

- Firefox
- Internet Explorer
- Chrome
Client Transactions Information

Installing the plugin adds the **Client Transactions** module to the **System Logs** application. It provides a list of every logged transaction between client and server within the last day:

### Client Transactions Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created</td>
<td>Moment the transaction was recorded.</td>
</tr>
<tr>
<td>Response Time</td>
<td>Number of ms spent by the server in fulfilling the transaction.</td>
</tr>
<tr>
<td>Business Rule Time</td>
<td>Number of ms spent by business rules triggered by the transaction.</td>
</tr>
<tr>
<td>SQL Time</td>
<td>Number of ms spent by the SQL database.</td>
</tr>
<tr>
<td>Client Response Time</td>
<td>(Load_completion_time) - (start_time). It is inclusive of server time.</td>
</tr>
<tr>
<td>Client Network Time</td>
<td>Number of ms spent by the network the client is connecting through.</td>
</tr>
<tr>
<td>Browser Time</td>
<td>Number of ms spent by the browser during the transaction.</td>
</tr>
<tr>
<td>Client Script Time</td>
<td>The number of ms spent executing client scripts.</td>
</tr>
<tr>
<td>UI Policy Time</td>
<td>Number of ms spent executing ui policy.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of transaction:</td>
</tr>
<tr>
<td></td>
<td>• Form</td>
</tr>
<tr>
<td></td>
<td>• List</td>
</tr>
<tr>
<td></td>
<td>• Other</td>
</tr>
<tr>
<td>Table</td>
<td>Name of table that appeared. For example, incident, change_request.</td>
</tr>
<tr>
<td>View</td>
<td>View for this form/list.</td>
</tr>
</tbody>
</table>

### Client Detailed Information

A more detailed breakdown of the client timings for all Form rendering (but not list rendering) is also tracked. To see details, drill into a particular client transaction record and observe the related list at the base of the screen.

### Client Detailed Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order</td>
<td>Order during the load in which this operation occurred.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of operation.</td>
</tr>
<tr>
<td>Name</td>
<td>Descriptive name of this particular operation</td>
</tr>
<tr>
<td>Duration</td>
<td>Number of ms this operation took to complete.</td>
</tr>
</tbody>
</table>
Components installed with Client Transaction Timings

The Client Transaction Timings plugin installs several components.

Database Table Structure

The plugin adds the table `syslog_client_transaction`.

Scripts

The plugin relies on the new script include `AJAXClientTiming`. This script gathers the information required and populates them on the `syslog_client_transaction` table.

Dependencies

This plugin does not require any other plugins, but does not gather information unless the Response Time Indicator `Response Time Indicator` is enabled.

Activating the Plugin

To activate the plugin, navigate to `System Definition > Plugins` and activate the plugin.

Note: New instances have the plugin activated by default.

Timing values

Timing values are broken down into several sections.

Client Transaction Timing

The variables in this diagram are defined as follows:
### Timing Values

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>start_time</td>
<td>Date and time the user requests a page (the user clicks on a link). This value is set by hooking into the <strong>beforeunload</strong> event of the previous page. WebKit browsers do not properly support the <strong>beforeunload</strong> event, which is why the client timings are not supported in Safari orChrome.</td>
</tr>
<tr>
<td>load_time</td>
<td>Date and time that the current page starts loading in the browser. An inline javascript that runs as the first script in the HTML body sets this value.</td>
</tr>
<tr>
<td>server_time</td>
<td>Time in ms spent by the server processing the transaction. The server reports this value to the client.</td>
</tr>
<tr>
<td>load_completion_time</td>
<td>Date and time that the page is fully rendered in the browser. This operation is performed as the last script on the page and identifies the time the page completed loading.</td>
</tr>
</tbody>
</table>

The following timings are reported at the bottom right of many forms and lists:

### Timing Values

<table>
<thead>
<tr>
<th>Label</th>
<th>Element</th>
<th>Description</th>
<th>Calculation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response Time</td>
<td>client_response_time</td>
<td>Overall time to deliver the page by subtracting the time the user requests the page from the time the page is fully rendered in the browser.</td>
<td>load_completion_time - start_time</td>
</tr>
<tr>
<td>Server Time</td>
<td>client_server_time</td>
<td>Time the server takes to process the transaction.</td>
<td>server_time</td>
</tr>
<tr>
<td>Network Time</td>
<td>client_network_time</td>
<td>Time the network takes to process the request. Calculated by subtracting the time of the user's request, from the time the page starts loading in the browser, and then subtracting the server processing time.</td>
<td>load_time - start_time - server_time</td>
</tr>
<tr>
<td>Browser Time</td>
<td>browser_time</td>
<td>Time the browser takes to deliver the page by subtracting the time the page is fully rendered from the time the page starts loading in the browser.</td>
<td>load_completion_time - load_time</td>
</tr>
</tbody>
</table>
Define a relative duration

You can define a relative duration to work out duration time for SLAs.

- From the left navigation pane, select **System Scheduler > Relative Durations**.

  Four base Relative Durations are available:
  
  - Two business days by 4pm
  - Three business days by 4pm
  - Next business day by 4pm
  - End of next business day

  **Note:** The business schedule you use defines business day durations. If you define no schedule, by default the durations are 24 X 7.

Look at the End of next business day Relative Duration. From the Relative Durations list, select the **End of next business day** Relative Duration. The variable `days` is set to one, because the result of this calculation should land one day in the future. The rest of the script is as in the screenshot. If desired, you can customize the time at which you want the Relative Duration to end (currently set to 5pm).

```javascript
// Next business day by 5pm
var days = 1;

calculator.calcRelativeDueDate(calculator.startDate, days, '17:00:00');
```

There is one more important Relative Duration design aspect that is used by the other three out-of-box Relative Durations. To illustrate this design let's look at **2 business days by 4pm**.

As you can see in the image, within the script there is an if-statement. This if-statement is checking to see if the calculated time is after 10am. If it is, then an extra day is added to the calculation. Hence the description of **2 business days by 4pm if before 10am.**
The "End of the business day" has nothing to do with the associated schedule. The end time of 17:00 is hard-coded into this Relative Duration script. If you want the time to be different than 5pm, you must change it in the script.

Use a relative duration

When you define an SLA, you can set the Duration type to be a relative duration.

When using relative durations, you can also use the Relative duration works on field. It calculates against the SLA record, or the task record that the SLA record is used for.

This example demonstrates how a relative duration of End of next business day works.

1. Create an SLA that has a relative duration of End of next business day.
2. Complete the rest of the fields of this SLA with the values as shown, also setting a Schedule and a Timezone if you want.
3. To show how this Relative Duration works, create a new incident. The SLA starts for this incident. If you look at the **Planned End Date** field, notice that the date is the next business day at 5pm (See image).

![Incident Details]

**Note:** Pause conditions are not compatible with Relative Durations.

---

**Search administration**

The Now Platform includes multiple search engines and interfaces to help users easily and quickly find the information they need.

**Search engines**

The Now Platform includes two search engines:

- **Zing text indexing and search engine**
  Default search engine which provides fast results and emphasizes relevancy scoring.

- **AI Search**
  Provides consumer-grade search capabilities for , , and .

**Search plugins**

These search plugins offer specialized search experiences for particular search contexts.

**Contextual Search**

The Contextual Search plugin enables search that focuses on query context and user intent to fetch the most relevant set of results. Contextual search displays related results within a form or record producer based on the text you enter in a field.
CMDB Search

The CMDB Search plugin enables users to query CMDB CIs and relationships through the global text search field. CMDB depends upon the Zing text indexing and search engine.

Search interfaces and widgets

These are search fields and widgets offered in the Now Platform UI or in Now Platform applications.

Global text search

The global text search field in the Now Platform UI enables search of multiple tables from a single search field.

Service Portal

The Service Portal framework displays search data within a widget on the search page.

Service Portal search widgets

Service Portal includes widgets for multiple forms of search.

Now Mobile app

The Now® Mobile app provides global text search, voice search, and photo search.

Mobile Agent

The Mobile Agent app enables service desk agents to promptly manage and resolve end user issues from their mobile devices.

Virtual Agent

The Virtual Agent platform uses search to help parse user statements and intents.

Agent assist

The Agent assist feature in Workspace automatically displays possible solutions for records that agents open.

Machine learning solutions for Search administration

Machine learning in Search administration helps to enhance business scalability and improve business operations for organizations.

Businesses face a challenge with growing volumes of data, in extracting meaningful information from a huge set of raw data, and in deriving meaningful business insights. Machine learning can serve as a solution to a variety of business complexities as its algorithm is built using historical data. It helps avoid duplicate and inaccurate data being entered into the database and enables businesses to compute and process information much faster.

Predictive Intelligence for Contextual Search

The Predictive Intelligence for Contextual Search capability uses machine-learning algorithms to search for Similar Incidents, Similar Knowledge Articles, Similar Open Incidents, and Similar Resolved Incidents.

Predictive Intelligence suggests related results to help you solve an issue or resolve a question.

The sources such as Similar Incidents, Similar Knowledge Articles, Similar Open Incidents, and Similar Resolved Incidents are available only when the Predictive Intelligence plugin (com.glide.platform_ml) and the Predictive Intelligence for Contextual Search plugin (com.snc.contextual_search_ml) are available.
Features of Search administration

Enable and configure Search administration features.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Top tasks</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zing text indexing and search engine</td>
<td>Index and search record data by table.</td>
<td>• Enable text indexing for a table • Zing can expand search results with synonyms • Zing can include attachments in search results</td>
<td>Active</td>
</tr>
<tr>
<td>Contextual search</td>
<td>Display search results on forms and record producers when users enter text in a field.</td>
<td>• Define a search context</td>
<td>Active</td>
</tr>
</tbody>
</table>

Search Suggestions

The Search Suggestions application displays possible search completions or results to users as they enter terms into a search field. Search Suggestions supports the Service Portal, Now Mobile, and Virtual Agent search applications.

Search Suggestions stores search strings entered by users in the Search Event [sys_search_event] table. It periodically runs the **Build Search Suggestions** script to convert these search strings into search and auto-complete suggestions and store them in the Search Suggestion [sys_search_suggestion] table.

Display search suggestions for Zing users

The Zing text indexing and search engine use Search Suggestions to provide search suggestions to users as they enter search terms. Search suggestions indicate possible completions of the user’s search query.

Zing displays search suggestions in the Service Portal and Now Mobile search applications.

**Note:** If either of these search applications has the AI Search engine enabled, it displays auto-complete suggestions instead, as described in the following section.

For more details on Zing search suggestions, see Zing displays search suggestions as users enter search terms.

Display auto-complete suggestions for AI Search users

The **AI Search** engine uses Search Suggestions to provide auto-complete suggestions to users as they enter search terms. Unlike search suggestions, auto-complete suggestions can include possible search results as well as possible search query completions.

Auto-complete suggestions appear in search applications that have AI Search enabled. These typically include Service Portal, Now Mobile, and Virtual Agent.

For details on AI Search auto-complete suggestions and instructions for configuring them in search applications, see Auto-complete suggestions in AI Search applications.
Search Suggestions rules

In both Zing and AI Search, suggestions offered by the Search Suggestions application obey the following rules:

• Suggestions are search source-specific. For example, if you use the Service Catalog homepage search feature in the Service Portal, you only receive suggestions generated from users who were also searching within the Service Catalog.
• Suggestions are interface-specific. For example, if you use the search feature in the Service Portal, you only receive suggestions generated from search queries in the Service Portal, not, for example, from Now Mobile. Each unique Service Portal has its own suggestions, and they are not shared with other portals.
• Suggestions are in the same language as the current user’s language.
• Suggestions for external users are not shared with internal users, and conversely.

Schedule the Build Search Suggestions script

Specify when to run the script that builds search and auto-complete suggestions from user search strings.

Role required: admin

Search Suggestions stores search strings entered by users in the Search Event [sys_search_event] table. The Build Search Suggestions script turns those search strings into search and auto-complete suggestions and stores them in the Search Suggestion [sys_search_suggestion] table.

By default, this script runs daily. You can customize how often and at what time the script runs. How often you run the script depends on how frequently you want to update suggestions for users. When you run the script might depend on performance considerations.

1. Navigate to Scheduled jobs and click Build Search Suggestions.
2. In the Scheduled Search Execution form, edit how often the script runs in the Run field.
3. Edit the time of day the script runs in the Time field.
4. Click Update.
5. Optional: Click Execute Now to run the script immediately.

Prevent the creation of suggestions in special cases

Disable generation of suggestions from specific search strings to keep expletives from appearing in search results or to prevent disclosure of personal or secure information.

Role required: admin

Search Suggestions generates search and auto-complete suggestions from the search strings that users enter. You may not want to create suggestions from all search strings. You can prevent the generation of suggestions using one of the following approaches:

• Exclude words or regular expressions from search and auto-complete suggestions.

For example, a user might search on KB2938272. This search string is too opaque to provide a meaningful suggestion. Or, someone might enter a social security number or phone number as search strings which should not be surfaced as suggestions to anyone else. So, you might exclude all search strings that contain multiple numbers. Likewise, if someone uses an expletive in a search string, you may not want to surface that word in suggestions. The Search Suggestion Exclusion List [sys_search_suggestion_blacklist] table contains the list of excluded words.

• Assign roles to users that prevent the generation of suggestions from their search strings.

There may be individuals whose searches should not appear in search or auto-complete suggestions for privacy or security reasons. To prevent their searches from generating suggestions, assign them the suggestion_exempt role.
This role is unnecessary in most situations. Search Suggestions never shows who performed the initial search. To prevent people from seeing search and auto-complete suggestions, assign them the cannot_read_suggestions role.

Search Suggestions comes with a table of excluded words and regular expressions in these languages:

- Chinese
- Czech
- Dutch
- Finnish
- French
- German
- Hebrew
- Hungarian
- Italian
- Japanese
- Norwegian
- Polish
- Portuguese
- Russian
- Spanish
- Swedish
- Thai
- Turkish

1. In a browser, navigate to https://<instance name>.service-now.com/sys_search_suggestion_blacklist_list.

2. To make a word or regular expression active or inactive:
   a) Click the term in the list that you want to activate or deactivate.
   b) In the Search Suggestion Exclusion List form that appears, select or clear the Active option.

3. To add a new excluded word or regular expression:
   a) Click New.
   b) On the form, fill in the fields.

**Search Suggestion Exclusion List form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phrase</td>
<td>Word or regular expression to exclude.</td>
</tr>
<tr>
<td>Language</td>
<td>The language that the excluded word is in. Use the ISO 639-1 code for the language, such as &quot;en&quot; for English. Because regular expressions work for all languages, search suggestions ignores this field for regular expressions.</td>
</tr>
<tr>
<td>Description</td>
<td>Explanation of why you excluded the word or regular expression if it's not obvious. This field is especially important for regular expressions.</td>
</tr>
<tr>
<td>Active</td>
<td>Option to remove the excluded word or regular expression from suggestions.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Type</td>
<td>Option that specifies whether the Phrase field represents one word or a regular expression.</td>
</tr>
</tbody>
</table>

**Note:** If you use regular expressions, you should verify that they exclude the words you want. For more information, see Test regular expressions in Search Suggestion Exclusion List entries.

4. To assign someone a role that prevents them from seeing search and auto-complete suggestions, or to prevent their search strings from becoming suggestions:
   a) Navigate to **User Administration > Users** and click the name of a user.
   b) In the Roles related list, click **Edit**.
   c) To prevent a user from seeing search and auto-complete suggestions, move **cannot_read_suggestions** from the Collections column to the Roles List column and click **Save**.
   d) To prevent a user's search strings from generating search and auto-complete suggestions, move **suggestion_exempt** from the Collections column to the Roles List column and click **Save**.

---

**Test regular expressions in Search Suggestion Exclusion List entries**

Regular expressions are powerful and often require editing to get the correct behavior. When using regular expressions to exclude search strings, test the expressions thoroughly so as not to have unintended results.

Role required: admin

The Exclusion List Rule and Search Suggestion Relations \([m2m\_blacklist\_search\_suggestion]\) table lists the suggestions eliminated from the Search Suggestion \([sys\_search\_suggestion]\) table by entries in the Search Suggestion Exclusion List \([sys\_search\_suggestion\_blacklist]\) table.

1. In your browser, navigate to https://<instance name>.service-now.com/m2m\_blacklist\_search\_suggestion\_list.
   A list of words excluded from search suggestions appears in the Exclusion List Rule and Search Suggestion Relations table. The Suggestion column shows the search string that was eliminated in the creation of suggestions.
2. Add a regular expression to the exclusion list table.
   For more information, see Preventing suggestions in special cases.
3. In a search field, for example, on the ServiceNow\® Service Portal, enter words that satisfy the regular expression.
4. Run the script that builds the search suggestions.
   For more information, see Schedule the Build Search Suggestions script. Click **Execute Now** to run the script immediately.
5. In the m2m\_blacklist\_search\_suggestion\_list table, click the menu icon (≡) for the Exclusion List column heading and then select **Group By Exclusion List** to see the regular expressions and what they eliminated.
6. Review the suggestions in the table to see if the regular expressions removed the suggestions they should have and no more.
7. In the sys\_search\_suggestion\_blacklist table, set an excluded regular expression's **Active** field to **false**, then run the Build Search Suggestions script again to make sure that only excluded suggestions were removed.
8. Revise the regular expressions if necessary and repeat the procedure.
Schedule suggestion pruning

Search Suggestions limits the number of search and auto-complete suggestions stored in the sys_search_suggestion table to 500,000. A periodic pruning job removes the least relevant suggestions and increases the overall relevancy of suggestions.

Role required: admin

By default, the pruning job runs once a week and limits the sys_search_suggestion table to 500,000 suggestions. Once the table reaches that limit, the pruning job removes the lowest-rated search and auto-complete suggestions to keep the maximum number of suggestions at 500,000. Pruning the least relevant suggestions improves the relevancy of the suggestions.

How often you run the pruning job might depend on how quickly you generate suggestions from the sys_search_event table, and how quickly the sys_search_suggestion table exceeds 500,000 suggestions.

1. Navigate to System Definition > Scheduled Jobs.
2. Edit the Prune Search Suggestions job.
3. On the form, edit the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run</td>
<td>Frequency of execution for the pruning job. To execute the job manually, select On Demand and click Execute Now.</td>
</tr>
<tr>
<td>Day</td>
<td>Day of the week to run the pruning job.</td>
</tr>
<tr>
<td>Time zone</td>
<td>Time zone to use when interpreting the Time field value.</td>
</tr>
<tr>
<td>Time</td>
<td>Time of day to run the pruning job. Specify hours (00–23), minutes (00–59), and seconds (00–59).</td>
</tr>
<tr>
<td>Repeat interval</td>
<td>Interval between executions of the pruning job when Run is set to Periodically. Specify days (01–07, where 01 is Sunday), hours (00–23), minutes (00–59), and seconds (00–59).</td>
</tr>
<tr>
<td>Conditional</td>
<td>Script to run when executing the pruning job.</td>
</tr>
</tbody>
</table>

Note: The fields on the form change with the choice of the Run value.

4. Click Update.

Setting historical limitations for generating suggestions

Limiting the number of search strings stored in the sys_search_event table limits how far back you can go to create search and auto-complete suggestions. Set the Auto Flush parameter to how far back in time you want to go.

Role required: admin

The sys_search_event table contains all of the strings used in searches. Scripts use this table to generate search and auto-complete suggestions. A system property sets the maximum age for records in the table. The default is 180 days. If you want to review analytics and generate search and auto-complete suggestions from search strings that are more than six months old, increase the number of days. Longer durations increase the size of the table and disk consumption.

1. In Filter Navigator, enter sys_auto_flush.list.
2. Search on *search and edit the sys_search_event record.
3. On the Auto Flush form, edit the **Age in seconds** value.
   The default is 15,552,000 seconds, which is 180 days.

### Analyze search relevancy

Analyze data from the Search Suggestions tables to understand how your users interact with search.

Role required: admin

Search Suggestions uses the following tables:

- **Search Event** [sys_search_event]: Stores all search strings and search results.
- **Search Source Event** [sys_search_source_event]: Stores search strings and search results and ties them to a data source, for example, the suggestion came from the knowledge base table rather than the catalog table.
- **Search Suggestion** [sys_search_suggestion]: Stores suggestions for searches.

For details on the Search Suggestions tables, see [Understanding Search Suggestions tables](#).

1. Display the Search Event [sys_search_event] table by navigating in your browser to `https://<instance name>.service-now.com/sys_search_event_list.do`.

2. In the **Number of results** column, find search queries that had zero results.
   A value of 0 means that someone searched but didn’t get any search results. You can choose to create information, such as a knowledge article, to provide search results in the future, create synonyms for the search words that would surface a search result, or not provide information if the question is irrelevant.

3. Average the numbers in the **Click Rank** column. Goal: the lower the better.
   Click rank shows which suggestion in the list of suggestions you selected. If you click the first suggestion in the list of suggestions, the click rank value is 1. If you click the 6th suggestion listed, the click rank value is 6. If you click multiple search results, the click rank is the highest listing value. For example, if you click the first listing, return to the search page and click the 6th listing, return to the search page and click the 4th listing and find an answer, the click rank is 6 (not 4). The goal is to reduce the average of these numbers, which indicates the top suggestions are the most relevant.

4. Determine the click-through-rate by dividing the number of records where the click rank is not zero by the total number of records. Goal: the higher the number, the better.
   Click-through-rate is a good indicator of how often users find relevant results, but it doesn’t reveal how much effort it took to find those results. That’s where click rank comes in. Click rank describes how much effort it took the user to find what they perceived to be a relevant result.

5. Average the numbers in the **Refinement** column. Goal: the lower the better.
   Refinement is the number of actions a user took to reduce the number of search results. Actions include sorting and filtering. More refinements means more effort to find relevant search results.


7. In the **Has results** column, find any search queries where the result is **false**.
   False means that someone searched but didn't get any search results from a particular source table, for example, the Knowledge Base table. You can choose to create information, such as a knowledge article, on the source to provide search results in the future, create synonyms for the search words that would surface a search result in that source table, or not provide information if the question is irrelevant.
**Understanding Search Suggestions tables**

Search Suggestions uses tables to generate relevant search suggestions. By understanding these tables, you can improve the relevancy of search suggestions in your system.

**Search Event table**

The Search Event [sys_search_event] table stores search strings and their search results.

**sys_search_event table**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search query</td>
<td>Search string that the user entered.</td>
</tr>
<tr>
<td>Has results</td>
<td>Boolean value that specifies whether the search did (true) or didn't (false) return results. For all false values, consider adding information so that the same search would return suggestions in the future.</td>
</tr>
<tr>
<td>Click rank</td>
<td>Click rank shows which suggestion in the list of suggestions you selected. If you click the first suggestion in the list of suggestions, the click rank value is 1. If you click the 6th suggestion listed, the click rank value is 6. If you click multiple search results, the click rank is the highest listing value. For example, if you click the first listing, return to the search page and click the 6th listing, return to the search page and click the 4th listing and find an answer, the click rank is 6 (not 4). The goal is to reduce the average of these numbers, which indicates the top suggestions are the most relevant.</td>
</tr>
<tr>
<td>User</td>
<td>User who performed the search.</td>
</tr>
<tr>
<td>Application ID</td>
<td>Application where the search feature was used, for example, you did a search in the Service Portal. See UI source.</td>
</tr>
<tr>
<td>Language</td>
<td>Language of the query. Search only returns suggestions that are in the same language as the search query.</td>
</tr>
<tr>
<td>Refinements</td>
<td>Number of actions that you took to reduce the number of search results. Actions include sorting and filtering. The goal is to reduce this number.</td>
</tr>
<tr>
<td>UI source</td>
<td>Specific screen (mobile) or page (portal) where the search query came from. See Application ID.</td>
</tr>
<tr>
<td>Session</td>
<td>ID of the session, which specifies when the search happened.</td>
</tr>
<tr>
<td>AI Search Profile</td>
<td>Name of the search profile used for the search. Only applicable for searches made with the AI Search engine.</td>
</tr>
</tbody>
</table>

**Search Event per source table**

The Search Event per source [sys_search_source_event] table stores records correlating search strings with results from a specific table, here called a data source. A search can query multiple tables. The sys_search_event table lists one record for the entire search, while the sys_search_source_event table lists one record for each data source (table) queried.
### sys_search_source_event

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search query</td>
<td>Search string that you entered.</td>
</tr>
<tr>
<td>Source</td>
<td>System ID of the data source. For example, the system ID of the Knowledge Base might be c45067sample3c82eef3e. Suggestions from one source are used as suggestions for that source only. For example, a suggestion derived from the Service Portal would not be used as a suggestion in Now Mobile.</td>
</tr>
<tr>
<td>Has results</td>
<td>Boolean value that specifies whether the source did (true) or didn't (false) supply search results. For all false values, consider adding information so that the same search query would return suggestions in the future.</td>
</tr>
<tr>
<td>Created</td>
<td>Time stamp of the search query.</td>
</tr>
</tbody>
</table>

### Search Suggestion table

The Search Suggestion [sys_search_suggestion] table stores search and auto-complete suggestions. A scheduled job uses the sys_search_event table to build the content of the suggestion table. This job segregates generated suggestions by source. Suggestions generated from searches on the Service Portal, for example, are only returned for other Service Portal searches. These suggestions are not returned for Now Mobile queries.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application ID</td>
<td>Application where the search feature was used, for example, you did a search in the Service Portal.</td>
</tr>
<tr>
<td>User group</td>
<td>Specifies whether an internal or external user generated the search query. Suggestions for internal users are not shared with external users and vice versa.</td>
</tr>
<tr>
<td>Language</td>
<td>Language of the query. Search only returns suggestions that are in the same language as the search query.</td>
</tr>
<tr>
<td>Score</td>
<td>Suggestion rank. The higher the score, the more relevant the suggestion. Once all suggestions are returned for a search query, the suggestions are sorted by Score, the highest listed first. Scores reflect how often you selected a suggestion. A popular suggestion implies that it answers the query.</td>
</tr>
<tr>
<td>Source</td>
<td>System ID of the data source. For example, the system ID of the Knowledge Base might be c45067sample3c82eef3e. Suggestions from one source are used as suggestions for that source only. For example, a suggestion derived from the Service Portal would not be used as a suggestion in Now Mobile.</td>
</tr>
</tbody>
</table>

### Domain separation and Search Suggestions

Domain separation is unsupported in the Search Suggestions application. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can control several aspects of this separation, including which users can see and access data.

**Support level: No support**

- The domain field may exist on data tables but there is no business logic to manage the data.
• This level is not considered domain-separated.

For more information, see Application support for domain separation.

Overview

Domain separation provides complete data isolation for domain-specific users.

How domain separation works with Search Suggestion

By default, Search Suggestion results are limited to the specific domain of the logged-in user. Search and auto-complete suggestions are not shared in parent or child domains.

Search signals

Search stores signal data from user searches. The aggregated signal data helps improve search result relevancy in your system.

Signals record details of user searches, search refinements, and interactions with search results.

AI Search machine learning relevancy analyzes aggregated signal data and automatically tunes search relevancy scoring to reflect user behavior patterns. This tuning helps improve result relevancy for search users.

To learn more about AI Search machine learning relevancy, see Machine learning relevancy in AI Search.

Understanding search signal tables

Search uses tables to store details from user searches, search refinements, and interactions with search results. These details are called search signals. Data from the search signal tables helps improve the relevancy of search results in your system.

Search signals refer to user, query, and similar data stored in columns on search suggestion tables. For a guide to search suggestion tables and their columns, see Understanding Search Suggestion tables.

Search Signal Event table

The Search Signal Event [sys_search_signal_event] table stores signal data produced when users submit a search.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browser</td>
<td>User browser agent string.</td>
</tr>
<tr>
<td>Latitude</td>
<td>Latitude coordinate of the user location in decimal degrees.</td>
</tr>
<tr>
<td>Longitude</td>
<td>Longitude coordinate of the user location in decimal degrees.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>First page results</td>
<td>JSON array of objects in which each node represents a single result returned in the first page of results for the search. The result order is preserved. Each object includes the unique record identifier (sys_id) of a result and the table where the result is located.</td>
</tr>
</tbody>
</table>

**Note:** The first page results are not updated when you refine a search.

---

**Search Signal Result Event table**

The Search Signal Result Event [sys_search_signal_result_event] table stores signal data for search results that users select.

### sys_search_signal_result_event

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Result DocID</td>
<td>The source table and record names for the selected search result.</td>
</tr>
<tr>
<td>Source Table</td>
<td>The source table for the selected search result.</td>
</tr>
<tr>
<td>AIS DocID</td>
<td>The source table name and record sys_id for the selected search result.</td>
</tr>
<tr>
<td>Result Type</td>
<td>The type of search result selected. For example, <strong>REGULAR</strong> for a regular search result or <strong>GENIUS</strong> for a Genius Result answer card.</td>
</tr>
<tr>
<td>Search Signal Event</td>
<td>Reference to the record for the search on the Search Signal Event [sys_search_signal_event] table.</td>
</tr>
</tbody>
</table>

---

**Search Signal Result Event Action table**

The Search Signal Result Event Action [sys_search_signal_result_event_action] table stores signal data for user interactions with search results.

### sys_search_signal_result_event_action

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signal Type</td>
<td>The type of user interaction signal recorded for the search result. For example, <strong>CLICK</strong> indicates that the user clicked a search result.</td>
</tr>
<tr>
<td>Signal Value</td>
<td>The value for the user interaction signal. For example, when the signal type is <strong>CLICK</strong>, the signal value is the numeric index for the search result that the user clicked.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Search Signal Result Event</td>
<td>Reference to the record for the search result on the Search Signal Result Event [sys_search_signal_result_event] table.</td>
</tr>
</tbody>
</table>

### Search Autocomplete Query Event table

The Search Autocomplete Query Event [sys_search_autocomplete_query_event] table stores signal data for auto-complete suggestions that users select from the search input field.

**sys_search_autocomplete_query_event**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selected Query</td>
<td>The auto-complete suggested query that the user selected in the search input field.</td>
</tr>
<tr>
<td>Click Index</td>
<td>The numeric index of the auto-complete suggestion that the user selected in the search input field.</td>
</tr>
<tr>
<td>Latitude</td>
<td>Latitude coordinate of the user location in decimal degrees.</td>
</tr>
<tr>
<td>Longitude</td>
<td>Longitude coordinate of the user location in decimal degrees.</td>
</tr>
<tr>
<td>Search Profile</td>
<td>Reference to the search profile used for the search query.</td>
</tr>
</tbody>
</table>

### Genius Result Event Action table


**sys_search_genius_result_event_action**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action Id</td>
<td>The identifier for this Genius Result event action signal.</td>
</tr>
<tr>
<td>Action Type</td>
<td>The type of action taken from the Genius Result answer card.</td>
</tr>
<tr>
<td>Card Type</td>
<td>The type of Genius Result answer card that the user interacted with.</td>
</tr>
<tr>
<td>Search Signal Result Event</td>
<td>Reference to the record for the Genius Result answer card on the Search Signal Result Event [sys_search_signal_result_event] table.</td>
</tr>
</tbody>
</table>

### Zing text indexing and search engine

Index and search record data by table.

The ServiceNow® Zing text indexing and search engine is the default search engine used to search Now Platform® record data. Its engine is created entirely with ServiceNow code and implemented within the relational model.
The Zing text search index is split into multiple database shards for parallel querying. Its search engine logic yields fast results and emphasizes relevancy scoring. Relevancy scores include frequency and proximity weighting. Scores also include weighting for specific indexed fields such as title, short description, and metadata.

Zing provides type-ahead search suggestions and Did you mean: global search suggestions.

Administrators and users with the ts_admin role can configure the following Zing text search settings:

- match relevance
- relevancy field weights for each indexed table
- global stop words
- stop words for each index
- synonym dictionaries for each table
- tables with attachment indexing

### Features of Zing text indexing and search engine

Enable and configure Zing text indexing and search engine features.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Top tasks</th>
<th>State</th>
</tr>
</thead>
</table>
| Zing indexes words                         | Index documents by dividing them into words. Depending on the languages your instance supports, a word may be a single character such as a Chinese or Japanese pictogram or a sequence of characters separated by spaces such as with Latin, Arabic, and Pinyin languages. | - Enable text indexing for a table
- Regenerate a text index for a table
- Configure tables to use the Japanese tokenizer | Active |
| Zing computes document scores using three components | Compute document scores based on the frequency, sequence, and weight of search terms in the document. | - Score search terms by inverse document frequency (IDF)
- Set the relative weight of a field | Active |
### Available search options

Zing offers users several search interfaces and search operators to conduct text searches.

#### Available search interfaces

<table>
<thead>
<tr>
<th>Search interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global text search</td>
<td>Find records in multiple tables from a single search field.</td>
</tr>
<tr>
<td>Lists</td>
<td>Find records in a list; search in a specific field (Go to), all fields (Search), or in a specific column.</td>
</tr>
<tr>
<td>Knowledge Base</td>
<td>Find knowledge articles.</td>
</tr>
<tr>
<td>Navigation filter</td>
<td>Filter the items in the application navigator.</td>
</tr>
<tr>
<td>Live feed</td>
<td>Filter, search, or sort messages in live feed.</td>
</tr>
</tbody>
</table>
**Search interface**

| UI pages | Create a custom UI page to search for records in a table. |

**Available search operators**

<table>
<thead>
<tr>
<th>Search operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boolean operators</td>
<td>Include or exclude search terms in global text searches.</td>
</tr>
<tr>
<td>Quotation marks</td>
<td>Filter search results to only include matches to an exact phrase consisting of one or more words.</td>
</tr>
<tr>
<td>Wildcard characters</td>
<td>Expand search results to match any non-space character. The system supports both single-character and multiple-character wildcards.</td>
</tr>
</tbody>
</table>

**Global text search finds records from multiple tables**

Search multiple record types from a single search field.

To perform a global text search, perform one of the following actions based on the UI version you are using.

<table>
<thead>
<tr>
<th>UI version</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>UI16</td>
<td>Click the search icon in the banner on the upper right of the System settings for the user interface (UI), and then enter the search term.</td>
</tr>
<tr>
<td>UI15</td>
<td>Enter the search term in the search box in the upper right of the UI15 banner frame and Edge buttons.</td>
</tr>
</tbody>
</table>

All UI versions also have a global text search keyboard shortcut. The `ui_global_text_search` UI Macro provides the global text search field.

By default, the system returns results for tasks, Live Feed, policy, people, places, knowledge, and catalog records.
Global text search displays results dynamically
Display global text search results for each table as Zing generates them.

Global text search results UI

Zing displays search results in a dedicated page consisting of these elements.

Elements of the global search results UI

<table>
<thead>
<tr>
<th>UI element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Search terms</td>
<td>The current search terms and a field to enter new search terms.</td>
</tr>
<tr>
<td>2. Total results</td>
<td>The total number of matching records.</td>
</tr>
<tr>
<td>UI element</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>3. Search group name</td>
<td>The name of the search group.</td>
</tr>
<tr>
<td>4. Preview of matching records</td>
<td>The partial list of matching records up to the preview limit. By default, the system displays up to 10 matching records per table, sorted from highest to lowest document score. The system displays a separate list for each table in the search group. By default, the system uses the table text_search list view if available. Otherwise, it displays fields with the default list view. Users with the admin role can set the preview results limit and the search results view from the global text search properties.</td>
</tr>
<tr>
<td>5. Table name</td>
<td>The name of the search group table and the number of matching records in the table. Click the link to launch a filtered list view based on the query. Users with the admin role can hide matching record counts by setting the <code>sn_global_searchui.hide_results_count</code> property to <code>true</code> in the System Properties table.</td>
</tr>
<tr>
<td>6. Table filter</td>
<td>The current filter applied to search results from this table. Pointing to the information icon displays a pop-up containing the search filter applied. See Add a search group for information on applying a table filter to a search group.</td>
</tr>
<tr>
<td>7. Progress bar</td>
<td>The current percentage of tables searched. The system hides this element after the search is complete.</td>
</tr>
<tr>
<td>8. Link to all table results</td>
<td>The link to see all matching records from the search group table. Click the link to launch a filtered list view based on the query.</td>
</tr>
<tr>
<td>10. Results summary</td>
<td>The list of search groups and tables with the number of search results per group and table. Click the table name to display the associated preview list results.</td>
</tr>
</tbody>
</table>

**Text search views format search results**

Configure how the system displays global text search results with a text search view.

Each search result listing consists of these elements.

1. **Number:** C:\G0000072 | **Type:** Normal | **State:** Authorize | **Planned start date:** 2017-05-19 19:30:00 | **Planned end date:** 2017-05-19 19:45:00
2. **Requested by:** System Administrator | **Assign to:** Bow Ruggeri
3. **We need to add additional redundant name servers to Linux100, Linux101 and PS LinuxApp01.**

**Sample search result listing**

© 2021 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Search result elements

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
<th>Matching criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Title</td>
<td>The title is the first line of the search result block. The title links to the matching record of the search result.</td>
<td>Global search uses the first string field in the text search view that is not the number field. If there is no matching string field or the contents of the field is empty, the system displays the text &quot;No title&quot; in the session language. For example, in the default incident table view the short description field meets the criteria to be the title.</td>
</tr>
<tr>
<td>2. Field list</td>
<td>The field list is the second line of the search results. The field lists contains a name-value pair for each field in the text search view separated by a pipe character. The system displays the field list in gray text.</td>
<td>All fields in the text search view that do not match the title or description criteria.</td>
</tr>
<tr>
<td>3. Description</td>
<td>The description is an optional third line of the search results. The system displays the description in black text.</td>
<td>Global search uses the first string field in the text search view that is not the title and is over 100 characters in length. If no field matches this criteria, the search results omit this line. For example, there is no matching description field in the text search view of the Incident table.</td>
</tr>
</tbody>
</table>

By default, the system uses the text_search list view to format global text search results. If a text_search view doesn't exist, the system instead formats search results using the default form view. Implementers can specify which view the system uses to format search results with the system property `glide.ui.text_search.view`.

**Search groups filter search results by table**

The system displays search results by search group, which are collections of related tables.

Within each search group, the system divides search results by table. A user must have read access to a table to see search results for it.

**Default search groups**

**Default system search groups**

<table>
<thead>
<tr>
<th>Search group</th>
<th>Example tables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tasks</td>
<td>Incident, Change Request, Problem</td>
</tr>
<tr>
<td>Live Feed</td>
<td>Live Feed Message</td>
</tr>
<tr>
<td>Policy</td>
<td>Business Rule, UI Policy, Client Script</td>
</tr>
<tr>
<td>People &amp; Places</td>
<td>User, Group, Location, Company</td>
</tr>
<tr>
<td>Knowledge &amp; Catalog</td>
<td>Knowledge Base, Service Catalog</td>
</tr>
</tbody>
</table>
Displaying search results by group

The system displays knowledge and service catalog search results within their respective search results pages. The system displays other results in list format.

For exact match searches, the system only returns records from the Task (task) and Knowledge (kb_knowledge) tables.

**Note:** The system filters global search results to display only knowledge articles that are in the same language as the preferred language setting.
Example global search results

Options for administrators

Administrators can customize these search groups settings for all users:

- Specifying which tables are part of the group.
- Specifying whether the search group is available for use.
• Specifying whether searches include results from this search group by default.
• Creating new search groups.

Enabling a search groups allows users to see records from the search group's tables. Disabling a search group hides records from the search group's tables.

Add a search group
You can add a search group to filter global search results.

Role required: text_search_admin

1. Navigate to System Definition > Search Groups.
2. Click New.
3. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name of the search group.</td>
</tr>
<tr>
<td>Roles</td>
<td>Select one or more user roles if you want to restrict access to the search group to those roles.</td>
</tr>
<tr>
<td>User group</td>
<td>Select a user group if you want to restrict access to the search group to users in that user group.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter text to display as a tooltip for the search group.</td>
</tr>
<tr>
<td>Active</td>
<td>Ensure the check box is selected to make the search group available.</td>
</tr>
<tr>
<td>Searched</td>
<td>Clear the check box if you want to exclude results from this search group by default. A user can manually choose to show results from this search group on the search results page.</td>
</tr>
<tr>
<td>Order</td>
<td>Enter a number to determine the order in which this search group is listed relative to other search groups.</td>
</tr>
</tbody>
</table>

4. Right-click the form header and select Save.
5. In the Text Search Tables related list, click New.
6. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>Select the table to search.</td>
</tr>
<tr>
<td>Active</td>
<td>Ensure the check box is selected to search the table.</td>
</tr>
<tr>
<td>Searched</td>
<td>Clear the check box if you want to exclude results from this table by default. A user can manually choose to show results from this table on the search results page.</td>
</tr>
<tr>
<td>Order</td>
<td>Enter a number to determine the order in which this table is listed relative to other tables in the search group.</td>
</tr>
<tr>
<td>Conditions</td>
<td>Select one or more conditions to determine which records on the selected Table are searched.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optional label</td>
<td>Enter the label to display for the table. For example, for a search group intended for your Sales team, display <strong>Contacts</strong> instead of Users for the User [sys_user] table.</td>
</tr>
</tbody>
</table>

7. Click **Submit**.
8. Add any other text search tables to include in the search group.

**Set global text search properties**

Administrators can control how global text search behaves with system properties.

**Role required: admin**

1. Navigate to **System Properties > Global Text Search**.
2. Set these properties.

**UI properties for global text search**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>glide.ui.text_search.enable</strong></td>
<td>Default value is true. Clear this option to disable the global text search capability.</td>
</tr>
<tr>
<td><strong>glide.ui.can_search</strong></td>
<td>Default value is itil, text_search_admin, admin. Add a role to enable it to use search.</td>
</tr>
<tr>
<td><strong>glide.ui.no_text_search</strong></td>
<td>Default value is sys_audit, sys_event, ecc_queue, ecc_event, syslog, syslog_transaction, sys_journal_field, sys_audit_relation, ecc_agent_log, ecc_mi_result, sysrule_escalate_history, sys_user_token, sys_time_dimension, sys_attachment_doc, sys_audit_delete. Tables that do not appear as options when defining search groups. Examples are system or maintenance tables.</td>
</tr>
<tr>
<td><strong>glide.ui.text_search.rowcount</strong></td>
<td>Default value is 10. Users can click through to see all results for a specific table.</td>
</tr>
<tr>
<td><strong>css.textsearch.kb.background.color</strong></td>
<td>This property only applies to the legacy global search results page. Default value is #FFFFDD.</td>
</tr>
<tr>
<td><strong>css.textsearch.catalog.background.color</strong></td>
<td>This property only applies to the legacy global search results page. Default value is #F0F7F9.</td>
</tr>
<tr>
<td><strong>glide.ui.text_search.match_view</strong></td>
<td>Default value is blank.</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
### Field

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.ui.text_search.view</td>
<td>List and form view to use for Global Text Search results. Blank means default view. Default value is the <code>text_search</code> view. If you do not have a <code>text_search</code> view, you can create it.</td>
</tr>
<tr>
<td>glide.ir.query_method</td>
<td>Query method for global text search. Run a query for each table, for each base class (parent table), against a single index regardless of table (requires text index regeneration), or let GlideRecord handle the query (simple). With the Zing text search engine, the preferred value is &quot;simple&quot;. Default value is Simple query.</td>
</tr>
<tr>
<td>glide.lucene.base_result_max</td>
<td>Maximum number of results that will be returned during a text index search. This limits the number of records that are extracted from the text index and appear. Default value is 100. This property is not supported by the Simple query method and is ignored.</td>
</tr>
<tr>
<td>glide.lucene.base_hits_max</td>
<td>Maximum number of entries that will be retrieved from the text index. Only the table that is involved will be returned from the text index for all entries that are between the value specified for maximum results and this value. This is done so that you can indicate that more results exists for any given table that are going to appear. Default value is 500. This property is not supported by the Simple query method and is ignored.</td>
</tr>
<tr>
<td>glide.ts.global_search.parallelism</td>
<td>Number of simultaneous processes (1 to 16) used when searching though multiple groups in a global search. Default value is 4. Each search group uses one thread to render results. Set this value to yield optimal results for your search group configuration. For example, if you have five search groups and four threads, the first four groups run in parallel and the fifth group starts when one of the first four groups finishes. This setup may work well if one of the groups is much larger than another. Similarly, if you have five search groups, setting this value higher than five yields no benefits.</td>
</tr>
</tbody>
</table>

3. Click **Save**.

The business rule **Text Search Property Change Rationally** validates the new values and aborts the update if they are outside its acceptable ranges.

4. **Open the System Properties table** and search for the property **glide.ts.max_wildcard_expansion**.

### UI properties for global text search

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>glide.ts.max_wildcard_expansion</td>
</tr>
<tr>
<td>Description</td>
<td>Maximum number of matches for a wildcard term that are allowed as unambiguous.</td>
</tr>
<tr>
<td>Type</td>
<td>Integer</td>
</tr>
<tr>
<td>Value</td>
<td>500</td>
</tr>
</tbody>
</table>
5. Edit the **Value**.
   If a wildcard search matches more words than this value, the system displays a message asking the user to refine the search.

6. Click **Update**.

7. To set the text search stemming language, install an internationalization (i18n) plugin.

8. Navigate to **System Properties > System Localization**.

9. Set this property.

### Text stemming property

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text Search stemming language</td>
<td>Default value is <strong>English</strong>. The system supports stemming in English, German, and French.</td>
</tr>
<tr>
<td>glide.ts.stemming_language</td>
<td></td>
</tr>
</tbody>
</table>

Enable the simple query method

Configure the simple query method to allow GlideRecord to handle queries and is supported by Zing Text Search.

1. Navigate to **System Properties > Global Text Search**.
2. Locate **Query method for global text search** (the glide.ir.query_method property).
3. Select **Simple query**.
4. Click **Save**.

The following properties are not supported:

- Maximum number of results that are displayed per table (glide.lucene.base_result_max)
- Maximum number of results counted per base class (glide.lucene.base_hits_max)

Configure parallel processing of search groups

To improve performance, only activate search groups and tables that are necessary to meet business needs.

For example, if you do not need Change Task results, deactivate that table in the Tasks search group. If only one group of users needs Change Task results, set up a separate search group that includes Change Tasks. Other users search using a group that does not contain Change Tasks.

Global text search can render results in parallel to improve performance. To configure the number of parallel processes:

1. Navigate to **System Properties > Global Text Search**.
2. Locate the property called **Number of simultaneous processes (1 to 16) used when searching through multiple groups in a global search**.
3. Enter the number of processes to run in parallel.
   Each search group uses one thread to render results. Set this value to yield optimal results for your search group configuration. For example, if you have five search groups and four threads, the first four groups run in parallel and the fifth group starts when one of the first four groups finishes. This setup may work well if one of the groups is much larger than another. Similarly, if you have five search groups, setting this value higher than five yields no benefits.
4. Click **Save**.

Enable or disable the junk filter
When its junk filter is enabled, Zing does not index or search for 2-digit numbers or single-character words (unless they are Chinese or Japanese characters). You can enable or disable the junk filter for individual tables.

For example, to disable matches for search terms like a or 40 in the Knowledge Base, turn on junk filtering for the kb_knowledge table.

1. Navigate to System Definition > Dictionary.
2. Open the dictionary entry for the table.
3. In the Attributes related list field, set the value of the Text index filter junk attribute:
   a) If you want Zing to include 2-digit numbers and single-character words when indexing and searching the table, set the attribute value to false.
   b) If you want Zing to ignore 2-digit numbers and single-character words when indexing and searching the table, set the attribute value to true.
4. Right-click the header and select Save.
5. Click the Generate Text Index related link and click OK.

**Note:**
- To have the desired effect, you may also need to reconfigure the automatic stop words. For example, if a specific 2-digit number appears in all of your problem numbers (92-0001, 92-0002, and so on), the automatic stop word threshold is quickly exceeded and the word is no longer found in searches. To find that 2-digit number in the problem table, you must disable both junk filtering and automatic stop words.
- Disabling the junk filter results in a larger table index. For optimal performance, do not apply this attribute unless it is required.

**Debug Zing**

Debugging messages create a log of search processes as they occur. These messages may help administrators configure optimal performance settings.

- To view debugging messages, navigate to System Diagnostics > Session Debug > Debug Text Search. The search log messages appear at the bottom of the results page for the remainder of your session.

**Debugging Messages**

- To debug text indexing problems, you may want to view text_index events in the system log.
In rare cases, you may need to reset the text search caches after regenerating a text index. If text search fails for known words, diagnose and fix this problem:

1. Enable text search debugging messages.
2. In any table with search problems, search for the problem text.
3. In the debug output, note the numbers used for the Stemmed terms.
4. Enter `ts_word.list` in the navigation filter.
5. Locate the stemmed terms and compare the numbers in the list to the debug output (Step 3). If the numbers are different, the UI node's cache is stale.
7. Click the Reset Text Search Caches related link and click OK.

Revert to the legacy global search UI
Disable the dynamic global search UI to preserve customizations you made to the legacy global search UI.

Role required: admin

1. Enter `sys_properties.list` in the Navigation filter.
2. The entire list of properties in the System Properties [sys_properties] table appears.
3. Click New.
4. Enter these field values.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>glide.ui.use_legacy_global_search</td>
</tr>
<tr>
<td>Type</td>
<td>true</td>
</tr>
<tr>
<td>Value</td>
<td>true</td>
</tr>
</tbody>
</table>

4. Click Submit.

The system displays the global search UI and uses the legacy display logic.

Legacy global search user preferences
The global text search results page allows users to set several user preferences for global text search.

The following search preferences are available from the Search tips and preferences link.
Search preferences

- Use remembered expand / collapse preferences
- In search group header, list tables with no search matches
- Show selectable search groups
- Show groups with no search matches
- Return task record if searching for exact number

Results are sorted by relevancy per table:
- computer AND Linux: Results contain both "computer" and "Linux"
- email OR network: Results contain either "email" or "network"
- server NOT Windows: Results contain "server" but not "Windows"
- "LDAP server is down": Results contain the phrase "LDAP server is down"
## Search preferences

<table>
<thead>
<tr>
<th>User preference</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Label</strong></td>
<td>Use remembered expand / collapse preferences</td>
</tr>
<tr>
<td><strong>Preference</strong></td>
<td>ts.remember.expanded</td>
</tr>
<tr>
<td></td>
<td>Specifies whether you want the collapse state of any search groups/tables remembered for your next search. If selected and you collapse the search results for the People &amp; Places search group for example, that group will be collapsed on your next search. If cleared, all groups and tables are expanded for every search.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Label</th>
<th>Show list of tables with no search matches</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Preference</strong></td>
<td>ts.show_negative_result_info</td>
</tr>
<tr>
<td></td>
<td>Specifies whether or not you want to see a summary of tables that had no search matches. For example: No matches for Requests, Catalog Tasks, Tickets.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Label</th>
<th>Show selectable search groups</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Preference</strong></td>
<td>ts.show_search_groups</td>
</tr>
<tr>
<td></td>
<td>Shows or hides the search group check box row.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Label</th>
<th>Show groups with no search matches</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Preference</strong></td>
<td>ts.show_empty_groups</td>
</tr>
<tr>
<td></td>
<td>Shows or hides a search group if it returns no matches. If selected, the search results display a placeholder row stating there were no matches for that group.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Label</th>
<th>Return task record if searching for exact number</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Preference</strong></td>
<td>ts.match</td>
</tr>
<tr>
<td></td>
<td>Shows or hides the full search results page if the search term matches a task record number. When selected, an exact match to a record number causes the system to hide the full search results and instead display the record with an exact match message. Exact search matches ignore most additional search conditions normally applied to the record such as the currently selected search groups or the knowledge article published state. For example, an exact search match for a knowledge article returns the article in any state as long as the current user has read access to it.</td>
</tr>
</tbody>
</table>

| Note: | The system filters exact search results to display only knowledge records that are in the same language as the preferred language setting. |
Global text search suggestions
Global text search offers two types of search suggestions.

The knowledge base and global text searches provide suggestions as you type. Type-ahead suggestions appear under the search box. Suggestions are based on similar searches that begin with the same characters.

Type-ahead search suggestions

The knowledge base and global text searches also provide suggestions for alternate search terms. Suggestions appear if your original search does not return any results and an alternate spelling or similar recent search does. For example, if you misspell a search term (such as eail), the correct spelling (email) may appear as an alternate search suggestion. Suggestions appear beneath the search box on the results page.

Alternate search suggestions

Note: The type-ahead search suggestions feature is only available in the UI15 interface.

Update a type-ahead suggestion

The knowledge base and global text searches provide suggestions as you type. These type-ahead suggestions are compiled on a nightly basis by a scheduled job.

Use the following procedure if you need to refresh this list sooner.

1. Navigate to System Scheduler > Scheduled Jobs.
2. Open TS Search Stats.
3. Run the scheduled job.

For more about how suggestions are generated and maintained, see the blog post Global Text Search Suggestions by a ServiceNow Technical Support Engineer in the Now Community.

Note: The type-ahead search suggestions feature is only available in the UI15 interface.

Configure a "Did You Mean?" suggestion

The Knowledge Base and global text searches can provide "Did you mean?" suggestions. Suggestions appear if a search does not return any results and an alternate spelling or similar recent search does. This feature is disabled by default.

1. Navigate to System Properties > Text Search.
2. Select any of the following check boxes:
   - **Suggest alternate search spellings for knowledge or global search** (the `glide.ts.dym.enable_spell_correct` property).
   - **Suggest related searches for knowledge or global search** (the `glide.ts.dym.enable_chain_suggest` property); uses search chains, which generate suggestions by tracking occurrences of similar searches, in order, over time.

   **Note:** The global search references in these check boxes only apply to the legacy global search functionality. They do not apply to the global search functionality introduced in the New York release, because the Did you mean? functionality is not available.

3. Click **Save**.

**List search finds records from the current table**

Search records from a table list view.

Indexed tables display the **for text** option in the list title bar, which searches all records for matching field values.
The list search field accepts **Boolean operators** (AND, OR, and NOT) in search queries. When a user adds a Boolean operator to a search query, the system only returns records that match all search conditions of the query.

The system also converts any search query into an equivalent keyword condition in the list breadcrumbs and filter. For example, searching for the text "Oracle OR SAP" produces the condition `[Keywords] [are] [Oracle OR SAP]`. The standard list controls can modify or remove these breadcrumbs and conditions.

**Boolean operators allow conditional search results**

Include or exclude search terms in global text searches.

All global text search interfaces support Boolean operators.

- Global text search field
- Knowledge Base search
- List search for text

**Note:** Boolean operators are case-sensitive. For example, **OR** is a Boolean operator while *Or* and *or* are search terms that may be stop words.
### Boolean operators

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OR or vertical bar symbol (|)</td>
<td>Finds a match if any of the terms exist in a document (a union using sets). For example, to find documents that contain either email password or just email, search for &quot;email password&quot; OR email or &quot;email password&quot;</td>
</tr>
</tbody>
</table>

When you use filter lists on keywords, OR and | produce the same results. For example, these two filters produce the same result by searching for records that contain either SAML or SSO:

*Searching with the OR operator*

However, using the .or. operator, which the system uses when you create OR condition groups for fields other than Keywords with the condition builder, can produce different results. For example, this filter searches for records with short descriptions containing SAML and then searches separately for records with short descriptions containing SSO:

*Searching with the pipe operator*
<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
</table>
| AND                          | Finds a match if all terms exist in a document (an intersection of sets). For example, to find documents that contain "CPU load" and "10 minutes", search for "CPU load" AND "10 minutes". By default, Zing applies an AND operator between all search terms regardless of whether the user entered them or not. For example, the system converts a search for the text "email server down" to [Keywords [are] [email] AND [Keywords [are] [server] AND [Keywords [are] [down].  

Note: For Knowledge Base searches, if the default AND search returns poor results, the search is automatically re-run with the OR operator. Administrators can configure the knowledge base search to always use OR by modifying the glide.knowman.search.operator system property. |
| NOT, minus (-), or exclamation point (!) | Excludes documents that contain the term after the NOT operator (a difference of sets). For example, to find documents that contain "CPU load" but not "10 minutes", search for "CPU load" NOT "10 minutes", "CPU load" -"10 minutes", or "CPU load" !"10 minutes". The NOT operator cannot be used with just one term. For example, the following search returns no results: NOT "10 minutes". NOT must be a stand-alone word. For example, atom NOT ion excludes the term ion. Whereas NOTION searches for the term notion. Minus and exclamation point must immediately precede the excluded term. For example, email !Joe excludes the term Joe but email ! Joe includes the term Joe. |

Quotation marks allow exact phrase searches

Filter search results to only include matches to an exact phrase consisting of one or more words.

Zing only matches documents that contain the exact words in the exact order you specify. An exact phrase search ignores:

- stop words
- punctuation marks
- wildcard characters

Note: Wildcard characters are ignored as punctuation.

For example, searching for the phrase "email password" returns the same search results as these phrases:

- "email the password" because the stop word "the" is ignored.
- "email password?" because the punctuation "?" is ignored.
*email password*" because the wildcard "*" is ignored as punctuation.

**Wildcard characters allow searching for patterns and variations**

Expand search results to match any non-space character. The system supports both single-character and multiple-character wildcards.

The following searches support wildcard characters.

- Global text search
- Knowledge Base

**Note:** To enable wildcard search in the Knowledge context, navigate to **Contextual Search > Search Contexts > Knowledge Base Search** and select the **Enable wildcard searches** check box.

- Search a list

**Note:** To perform a wildcard text search of a list, you must select **for text** as the search field. If you select a list field instead of **for text**, wildcard characters in search terms will be interpreted as list search wildcards.

- Reference fields

To perform a single-character wildcard search, use the percent sign (%) character. This wildcard finds words that contain any one character in place the percent-sign-character. For example, to find words such as **text** or **test**, search for **te%t**.

To perform a multiple-character wildcard search, use the asterisk (*) character. This wildcard finds words that contain zero or more characters in place of the asterisk-character. For example, to find words such as **planned** or **placed**, search for **pl*d**.

You can use wildcard characters anywhere in a search string, and can include multiple wildcards in the same word. For example, to find words including **affordable**, **effort**, and **offering**, search for **%ff%r***.

If a wildcard search returns too many hits, the system displays a message asking you to refine the search. Administrators can set a global text search property to change the limit for wildcard search results.

**Note:** Wildcard text searches are only effective with multiple character words. A wildcard within a sequence of pictogram characters returns too many options for an efficient search. Wildcards are best used with letter-based words.

**Zing generates search results in four phases**

Generate search results by dividing documents among shards, searching shard documents, scoring shard documents, and merging scores into an index.

Zing generates search results in four phases:

1. Divide searchable documents among index shards.
2. Search and filter shard documents.
3. Score shard documents.
4. Merge shard document scores into an index.
Phase 1: Divide searchable documents among index shards

When a search is executed, the system equally divides all searchable documents among 10 index shards. Each shard has a unique list of documents.

To maximize search efficiency, the system creates 10 query threads to simultaneously search each index shard.

Phase 2: Search and filter shard documents

Each query thread searches through its list of shard documents to identify documents that match the search criteria. For example, if you search for "wifi network," the system returns all documents containing both "wifi" and "network" in no particular order.

**Note:** A multiple word search is equivalent to multiple single word searches connected by an AND operator. For example, `[contains][wifi][AND][contains][network].`
The query thread assigns each matching document a numeric value (a document ID) to uniquely identify it. All other documents are ignored.

**Phase 3: Score shard documents**

The query thread scores each matching shard document.
Query threads search, filter, and score shard documents

1. Query Thread 0
   - Searches Shard 0
     - Filters Shard 0
       - Scores Documents in Shard 0

2. Query Thread 1
   - Searches Shard 1
     - Filters Shard 1
       - Scores Documents in Shard 1

   ... (Repeat for queries 2 to 9)

3. Query Thread 9
   - Searches Shard 9
     - Filters Shard 9
       - Scores Documents in Shard 9

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Phase 4: Merge and sort shard document scores

The system merges the document scores into a single index and sorts the documents from highest to lowest document score. The documents with the highest document score are most relevant to the search query.
Zing filters search results with access controls

Zing filters search results to only display records the user can access.

For example, suppose you index the System Properties [sys_properties] table. When the ITIL User searches for a term in the system properties table, Zing returns no search results because the ITIL user does not meet the ACL rule requirements.

ITIL User Search

When a system administrator searches for the same property, Zing returns search results from the System Properties tables because the administrator meets the ACL rule requirements.
Zing computes document scores using three components

The Zing search engine computes document scores based on the frequency, sequence, and weight of search terms in the document.

Document scores

The components of a document score for a search query are:

• Frequency: how often the search terms appear in the document.
• Sequence: how often the search terms appear in the same order as the search query.
• Weight: how heavily weighted the source field is in which the search terms appear.

Sample document score computation
Frequency points

Zing awards one point whenever a search term appears anywhere in the document. For example, when searching for distributed database server, a document that contains distributed three times, database five times, and server 17 times would have 25 frequency points.

To increase search result scores of search terms that appear more frequently in a document, but less frequently in a document set, you can Score search terms by inverse document frequency (IDF). When TF-IDF is enabled, search term scores are calculated by multiplying the term frequency score by the inverse document frequency score. Because enabling TF-IDF increases the weight of less common search terms, search results for that table are more likely to be relevant. For example, when searching for distributed database server, the term distributed might receive a higher score than server if it appears frequently in one document but less frequently in the document set as a whole.

Zing applies a multiplier to frequency points based on the value of the ts_weight attribute for the field in which the search term appears. A field with a text search scoring weight of 30 (ts_weight=30) would add 30 points for each inclusion of a search term.

Sequence points

Zing awards a document more points when it contains the search terms in the same order in which they were typed. The more search terms in sequence there are, the exponentially higher the score becomes. Zing awards sequence points as 10^x, where x is the number of search terms that appear in sequence.

In the distributed database server search example, Zing awards a document 100 (10^2) sequence points for each time it includes the two-term string database server. Likewise, Zing awards a document 1000 (10^3) sequence points each time it includes the three-term string distributed database server.

Zing applies a multiplier to sequence points based on the value of the ts_weight attribute for the field in which the sequence appears. The sequence points use the calculation (10^x * field ts_weight attribute).

Field scoring weights

The system elevates the default scoring weight of Knowledge record numbers, Knowledge short descriptions and metadata, task record numbers, and task short descriptions. Default ts_weight attributes for these fields are as follows:

- kb_knowledge.number = 50
- kb_knowledge.short_description = 10
- kb_knowledge.meta = 10
- task.number = 50
- task.short_description = 10

All other fields have a default ts_weight attribute of 1. The maximum possible weight value is 255.

Score search terms by inverse document frequency (IDF)

Enable term frequency–inverse document frequency (TF-IDF) to increase the search result scores of search terms that appear more frequently in a document, but less frequently in the whole collection of searchable documents.

Role required: admin

To enable TF-IDF scoring, a text index must be present for the table. Make sure that text indexing is enabled for the table before changing the query mode. See Enable text indexing for a table.

Administrators can enable TF-IDF scoring on a table to improve search results. The Knowledge table [kb_knowledge] has TF-IDF scoring enabled by default.
1. Navigate to the system dictionary and open the entry for the desired table.
2. In the Attributes related list, click New.
3. In the Attributes field, select Text search Enable IDF.
4. Click Submit.
The Enable IDF Score check box in the table's text index record can now be configured.
5. Navigate to System Definition > Text Indexes.
6. Open the text index created for the table.
7. Select Enable IDF Score.
   Regenerating document frequency is a one-time task. Regenerate document frequency when TF-IDF scoring is first enabled for a table.
9. Configure the desired notification and click OK.

Set the relative weight of a field

To improve search results, the Zing search engine assigns to each potential match a numeric score that represents its relevancy to the query.

Role required: admin

Administrators can control the relative importance of a match for each field in a table with the ts_weight attribute. The default weight of a field is 1.

1. Open the system dictionary entry for the field.
2. In the Attributes field, enter ts_weight=<value>, where <value> is the relative weight of the field.
   The following fields have elevated scoring weights by default:
   - kb_knowledge.number = 50
   - kb_knowledge.short_description = 10
   - kb_knowledge.meta = 10
   - task.number = 50
   - task.short_description = 10

   For example, if the Title field has a ts_weight=50 and the Description field has a ts_weight=10, then a match in the title is weighted 5 times more relevant than a match in the description and 50 times more relevant than a field without the ts_weight attribute.
3. Click Update.

   Note: To view the complete scoring system, see Document Scoring.

Zing indexes words

Index documents by dividing them into words. Depending on the languages your instance supports, a word may be a single character such as a Chinese or Japanese pictogram or a sequence of characters separated by spaces such as with Latin, Arabic, and Pinyin languages.

Zing uses spaces to define the basic unit of word separation. Zing uses the following rules to index words.
### Zing word indexing rules

<table>
<thead>
<tr>
<th>Rule</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Punctuation</td>
<td>Zing indexes some punctuation marks as part of some words to improve search results for common search terms. Zing converts any non-indexed punctuation characters to spaces. See Zing indexes punctuation as part of some words.</td>
</tr>
<tr>
<td>Pictograms</td>
<td>Zing supports the full range of Unicode pictogram characters. Each Chinese or Japanese pictogram is indexed as a separate word as if it were a single Latin-1 character surrounded by spaces.</td>
</tr>
<tr>
<td>Letter</td>
<td>Zing treats Latin-1, Arabic, and Pinyin characters as individual letters of space-separated-words. Sequences of letters define indexable words.</td>
</tr>
</tbody>
</table>

### Zing indexes punctuation as part of some words

Zing indexes some punctuation marks as part of some words to improve search results for common search terms.

#### Punctuation indexed as part of a word

<table>
<thead>
<tr>
<th>Punctuation</th>
<th>Indexed to find</th>
<th>Search behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ampersands [&amp;]</td>
<td>Company names</td>
<td>Zing locates terms containing punctuation characters that are common in company names: ampersands (&amp;), plus signs (+), or hyphens (-). For example, a search for H&amp;R Block locates exact matches to the search term.</td>
</tr>
<tr>
<td>Apostrophes [']</td>
<td>Proper names</td>
<td>Zing ignores trailing possessives and retains most others to find company names. For example, a search for O'Reilly's locates matches to O'Reilly and O'Reilly's.</td>
</tr>
<tr>
<td>Hyphens [-]</td>
<td>Company names</td>
<td>Zing locates terms containing punctuation characters that are common in company names: ampersands (&amp;), plus signs (+), or hyphens (-). For example, a search for Coca-Cola locates exact matches to the search term.</td>
</tr>
<tr>
<td>Product numbers</td>
<td>Zing locates product numbers that follow a typical pattern. To meet this pattern, search terms must contain frequent numbers and only include underscores (_), hyphens (-), or periods for punctuation. For example, a search for PROD-10-987 locates exact matches to the search term.</td>
<td></td>
</tr>
<tr>
<td>Numbers [123]</td>
<td>Product numbers</td>
<td>Zing locates product numbers that follow a typical pattern. To meet this pattern, search terms must contain frequent numbers and only include underscores (_), hyphens (-), or periods for punctuation. For example, a search for PROD10987 locates exact matches to the search term.</td>
</tr>
<tr>
<td>Punctuation</td>
<td>Indexed to find</td>
<td>Search behavior</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Record numbers</td>
<td>Zing locates record numbers that follow a typical pattern. To meet this pattern, search terms must start with a recognized record number prefix. For example, a search for INT1234567 locates exact matches to the Incident record.</td>
<td></td>
</tr>
<tr>
<td>Periods [.]</td>
<td>Acronyms</td>
<td>Zing locates acronyms whether they are separated by periods or not. For example, a search for u.s.a. locates matches to usa or u.s.a.. Note that wildcard searches may affect acronym handling. In another example, a search for u.s.* may yield better results than a search for u.s.a.*.</td>
</tr>
<tr>
<td>Host names</td>
<td>Zing locates sequences of letters and numbers separated only by periods. For example, a search for en.myhost123.com locates exact matches to the search term.</td>
<td></td>
</tr>
<tr>
<td>IP addresses</td>
<td>Zing locates numbers that follow a typical IPv4 address pattern. For example, a search for 10.0.0.1 locates exact matches to the search term.</td>
<td></td>
</tr>
<tr>
<td>Product numbers</td>
<td>Zing locates product numbers that follow a typical pattern. To meet this pattern, search terms must contain frequent numbers and only include underscores (_), hyphens (-), or periods for punctuation. For example, a search for PROD_10_987 locates exact matches to the search term.</td>
<td></td>
</tr>
<tr>
<td>Plus signs [+]</td>
<td>Company names</td>
<td>Zing locates terms containing punctuation characters that are common in company names: ampersands (&amp;), plus signs (+), or hyphens (-). For example, a search for Google+ locates exact matches to the search term.</td>
</tr>
<tr>
<td>Underscores [_]</td>
<td>Product numbers</td>
<td>Zing locates product numbers that follow a typical pattern. To meet this pattern, search terms must contain frequent numbers and only include underscores (_), hyphens (-), or periods for punctuation. For example, a search for PROD_10_987 locates exact matches to the search term.</td>
</tr>
</tbody>
</table>

**Note:** The punctuation handling described here does not affect wildcard and boolean operators. These operators provide separate Zing functions.
Zing indexes some HTML elements

Zing indexes the contents of certain HTML elements to improve document search results. This indexing is addition to the normal indexing by word.

**Indexed HTML elements**

<table>
<thead>
<tr>
<th>HTML element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title attribute</td>
<td>Zing indexes the contents of the <em>title</em> attribute of any HTML element. This is separate from the <em>title</em> element, which Zing already indexes when identifying the words of the document.</td>
</tr>
<tr>
<td>Anchor link target</td>
<td>Zing indexes the target URL specified in the <em>href</em> attribute of any anchor element.</td>
</tr>
<tr>
<td>Alt text for an image</td>
<td>Zing indexes the alternative text of any image element.</td>
</tr>
</tbody>
</table>

**Enable text indexing for a table**

Administrators can enable text indexing on a table to allow users to search for string values from table records.

Role required: admin

By default, the system creates text indexes for the tables with a Text index record (*System Definition > Text Indexes*). For example:

- Knowledge-related tables
- Core-data-related tables
- Connect-related tables
- Task table
- User table

**Note:** Whenever you create an index table, the system also creates Access Control Roles (ACLs) for new tables.

Text indexing can be a resource-intensive task that may take a while to complete. You may notice performance degradation or incomplete search results during index generation. To estimate text indexing duration, you can view historical statistics.

**Note:**

New tables created by update set transfers have text indexing disabled, even if it is enabled for the tables included in the update set.

To enable users to search tables created by update set transfers, you must manually enable text indexing for those tables.

1. Navigate to *System Definition > Dictionary*. 
2. Click the table name to open the dictionary entry.

A table in the System Dictionary is a record that has a **Table** name but no **Column name**.

![Dictionary Entry](image)

The `sys_user` table has no Column name.
3. Select the **Text index** check box to enable text indexing for text fields on the table.

4. Click **Update**.

5. Click **Generate Text Index**.

   The system schedules the table for text indexing, typically within a minute.

The Search **for text** option appears on the list view for the table.

- **Fields excluded from text indexing**
  - Text indexing excludes fields that meet certain name, type, attribute, or encryption conditions. User searches do not match or return values from excluded fields.

Text indexing excludes a field if it meets any of the conditions in the following table.

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field name</td>
<td>Text indexing includes the <strong>sys_class_name</strong> and <strong>sys_tags</strong> fields but excludes all other fields whose names begin with <strong>sys_</strong>.</td>
</tr>
<tr>
<td>Field type</td>
<td>Text indexing excludes fields of these types:</td>
</tr>
<tr>
<td></td>
<td>- Date</td>
</tr>
<tr>
<td></td>
<td>- Date/Time</td>
</tr>
<tr>
<td></td>
<td>- Duration</td>
</tr>
<tr>
<td></td>
<td>- True/False</td>
</tr>
<tr>
<td></td>
<td>- Workflow</td>
</tr>
<tr>
<td></td>
<td>For more information on these types, see <strong>Field types</strong>.</td>
</tr>
</tbody>
</table>
Configure a single table for indexing and searching

Configure a table with search attributes to index it.

Role required: admin, ts_admin

1. Navigate to **Text Index Configurations** and click **New**.
2. In **Applies to**, select **Table**.
3. In **Table**, select a table to configure.
4. Optional: Upgrade the indexing format to V4 if you intend to use this table in multi-table searches or if you want to use the BM25 scoring algorithm on this table.
   a) If the value in **Format** is not grayed out, you can select the indexing format, for example, V4, click **Submit**, and skip to step 5.
   b) If the value in **Format** is grayed out, the table has already been indexed. To reformat an indexed table, click **Submit**.
   c) Navigate to **Text Index Configurations** and click the table you submitted.
   d) Under **Related Links**, click **Show index name record**.
   e) Under **Related Links**, click **Upgrade to V4** and click **Submit**.

The specified table's indexing is upgraded from V3 to V4. Now, this table can be part of multiple-table indexing and BM25 is used to score the table's relevance score. Optionally, click **Show Configuration** under **Related Links** to show the table indexing format on the **Text Index Configuration** page.

5. Configure the indexing and search attributes on the selected table.
   a) Navigate to **Text Index Configurations** and click the table you configured.
   b) On the **Text Index Table Attribute Maps** tab, click **New**.
      Attributes either pertain to the way Zing indexes documents or ranks documents returned in search results.
   c) On the Text Index Table Attribute Maps form, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>Table to define attributes for.</td>
</tr>
<tr>
<td>Attribute name</td>
<td>Search engine attribute. For a list of the attributes and valid values, see Zing index and search attributes.</td>
</tr>
<tr>
<td>Value</td>
<td>Value for attribute.</td>
</tr>
</tbody>
</table>
e) Under Related Links, click Generate Text Index.

6. Configure column-level attributes.
   a) Navigate to Text Index Configurations and click a table.
   b) On the Text Index Column Attribute Maps tab, click New.
   c) On the form, fill in the fields. In Table, select a table to define attributes for. Only tables in the index group and their child tables display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>Table that contains the column you want to define attributes for.</td>
</tr>
<tr>
<td>Attribute name</td>
<td>Attribute. For a list of the attributes and valid values, see Zing index and search attributes.</td>
</tr>
<tr>
<td>Column</td>
<td>The name of the column in the selected table you want to apply the search attribute to.</td>
</tr>
<tr>
<td>Value</td>
<td>Value for attribute.</td>
</tr>
</tbody>
</table>

d) Click Submit.

e) Repeat this procedure to define additional search engine parameters for table columns in the index group.

f) Under Related Links, click Generate Text Index.

7. Optional: Add stop words.
   Stop words are words that you do not want to index, such as the, or, an. There is a global list of common stop words. So, you only have to add stop words specific to your situation. To see the global list of stop words, navigate in your browser to https://<instance name>.service-now.com/ts_stop_list.do.
   a) On the Index Stop Words tab, click New.
   b) In Index, select the index to add the stop word to.
   c) In Word, enter a single word you don't want to index and click Submit.

   Specifying a synonym dictionary searches on the search term as well as synonyms of the search term, such as car, and its synonym, auto. Zing provides a default synonym dictionary.
   a) On the Index synonym Dictionaries tab, click New.
   b) In Index, select the index to add the stop words to.
   c) In Synonym dictionary, select the synonym dictionary to use on the specified table.
      To add a dictionary, click New and follow the procedure in Create synonym dictionaries.

You have configured this table with an indexing format and attributes for indexing and searching. Now, you can search the table using glideRecord.addQuery(name, value), or glideRecord.addEncodedQuery(name, value). For more information about searching, see Querying tables in script.

Configure multiple tables for indexing and searching

Update tables to the V4 indexing format to include them in multiple table searches.

Role required: admin, ts_admin
Performing searches across multiple tables requires normalizing the tables first so the relevance scores mean the same thing for all tables. V4 indexing provides that normalization. Zing uses the Okapi BM25 ranking function to calculate the relevancy score of search results.

The V4 table indexing format is optimized for documentation, such as knowledge base articles. You do not need to reindex tables that use this format when you change the value of an indexing attribute, such as the weight of a field. If you want to use the BM25 ranking function on a single table, you can convert it to the V4 format.

To search across multiple tables, you:

1. Configure all of your chosen tables to use the V4 index format if they do not already use it.

   Note: In new instances, the Catalog Item [sc_cat_item], Knowledge [kb_knowledge], Social Q&A Questions [kb_social_qa_question], and User [sys_user] tables use the V4 index format. If you upgrade your instance from a previous release, the indexing format of these tables remains the same as it was in the older release.

2. Add the tables to an index group so they can be indexed and searched together.

   Note: You cannot add the Task [task] table or any tables that extend it to an index group.

3. Perform the search using `glideRecord.addQuery(name, value)` or `glideRecord.addEncodedQuery(value)`, where `name` is the special value 123TEXTINDEXGROUP321. For more information about searching, see Querying tables in script.

   1. Configure the tables that you want to include in multiple table searches to use the V4 index format.

      Note: Upgrading from V3 to V4 is easy. Downgrading from V4 to V3 is more difficult and discouraged.

      a) Navigate to System Definition > Text Index Configurations.
      b) Edit the record for the table that you want to upgrade to the V4 index format.
      c) If Format is not disabled, select V4, click Submit, and skip to step 2.
         You can choose index formatting in this step because no index exists for the table.
      d) If Format is disabled, an index already exists for the table and you must explicitly update the index format.
         Click the Show index name record related link.
         The Text Index page displays.
      e) Click the Upgrade to V4 related link, then click OK.
         The system schedules a task to upgrade the text index from V3 to V4, enabling this table to participate in multiple-table indexing.

2. Create an index group that specifies the tables you want to index together so you can search them together.

   a) Navigate to System Definition > Text Index Groups.
   b) Click New.
   c) Enter the following field values:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>Name for the group of tables that you want to index and search together.</td>
</tr>
</tbody>
</table>
You can add tables formatted with V3 and V4 to index groups. If you add V3 tables, the index group remains inactive.

d) Click **Submit**.

3. Configure the indexing and search attributes on tables in an index group.
   a) Navigate to **System Definition > Text Index Configurations**.
   b) Click **New**.
      The Text Index configuration form displays. If you already have an index group in the list, skip to step 3.d.
   c) In **Applies to**, select **Index Group**.
   d) In **Index group**, click the magnifying glass and select the index group you created, then click **Submit**.
      The only index groups that display are the ones you have already created.
      The Text Index Configuration table displays.
   e) Edit the record for your index group.
   f) On the **Text Index Table Attribute Maps** tab, click **New**.
      The Text Index Table Attribute Map form displays. Attributes pertain to the way Zing indexes or searches individual tables in the index group.
   g) In **Table**, select a table to define attributes for.
      Only tables in the specified index group and their child tables display.
   h) In **Attribute name**, click the magnifying glass and select an attribute.
      To see the list of attributes, enter `ts_configuration_attribute.list` in the application navigator. For attribute definitions, see **Zing index and search attributes**.
   i) In **Value** enter a value and click **Submit**.
      Valid values depend on the attribute. For information on valid values, see **Zing index and search attributes**.
   j) Repeat this procedure to define additional search engine parameters for other tables in the index group.
   k) Under **Related Links**, click **Generate Text Index**.
4. Configure search parameters on individual table columns in the index group.
   a) Navigate to **System Definition > Text Index Configurations**.
   b) Edit the record for your index group.
   c) On the **Text Index Column Attribute Maps** tab, click **New**.
      The Text Index Column Attribute Map form displays. Attributes pertain to the way Zing indexes or
      searches individual table columns in the index group.
   d) In **Table**, select a table to define attributes for.
      Only tables in the index group and their child tables display.
   e) In **Attribute name**, select a search engine parameter, enter a value for that parameter in **Value**, and click **Submit**.
      To see the list of attributes, enter `ts_configuration_attribute.list` in the application
      navigator. For attribute definitions, see **Zing index and search attributes**.
   f) In **Column**, specify the name of the column in the selected table you want to apply the search attribute to.
   g) In **Value**, specify the attribute's value that governs the search.
   h) Click **Submit**.
   i) Repeat this procedure to define additional search engine parameters for table columns in the index group.
   j) Under **Related Links**, click **Generate Text Index**.

5. Optional: Add a synonym dictionary.
   Specifying a dictionary enables searches on the search term and synonyms of the search term, such as **car** and
   its synonym **auto**. Zing provides a default synonym dictionary.
   a) Navigate to **System Definition > Text Index Configurations**.
   b) Edit the record for your index group.
   c) On the **Index synonym Dictionaries** tab, click **New**.
   d) In **Index**, select the table index to add the stop words to.
   e) In **Synonym dictionary**, select the dictionary to use.
      To add a dictionary, click **New** and follow the procedure in Create synonym dictionaries.
   f) Click **Submit**.
   g) Under **Related Links**, click **Generate Text Index**.

6. Click **Update**.

Perform the search using `glideRecord.addQuery(name, value)` or
`glideRecord.addEncodedQuery(value)`. For more information about searching, see Querying tables in
script.

**Zing index and search dictionary attributes**

The following dictionary attributes either affect the way Zing indexes tables or ranks search results.

**Index and search dictionary attributes**

Zing uses dictionary attributes set at the table or field level to configure the following settings:

- indexing behavior
- ranking of search results
- the BM25 relevancy ranking algorithm

### Zing index and search dictionary attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Data Type</th>
<th>Applies To</th>
<th>Applies to V3 or V4</th>
<th>Description</th>
<th>Label</th>
<th>Needs re-indexing?</th>
<th>Root Table Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>attachment_index</td>
<td>boolean</td>
<td>Table</td>
<td>Both</td>
<td>If true, attachments on the table are indexed for search purposes.</td>
<td>Attachment Index</td>
<td>TRUE</td>
<td>FALSE</td>
</tr>
<tr>
<td>no_text_index</td>
<td>boolean</td>
<td>Both</td>
<td>Both</td>
<td>This attribute on a field prevents the field from being included in a text index.</td>
<td>No Text Index</td>
<td>TRUE</td>
<td>FALSE</td>
</tr>
<tr>
<td>text_index_attachment_body_weight</td>
<td>float</td>
<td>Table</td>
<td>V4</td>
<td>Specifies how much consideration (weight, a float value) to give a search term found in the body of an attachment.</td>
<td>Text Index Attachment Body Weight</td>
<td>FALSE</td>
<td>TRUE</td>
</tr>
<tr>
<td>text_index_attachment_displayed</td>
<td>boolean</td>
<td>Table</td>
<td>Both</td>
<td>Displays attachments in text search results.</td>
<td>Text Index Attachment Displayed</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>text_index_attachment_title_weight</td>
<td>float</td>
<td>Table</td>
<td>V4</td>
<td>Specifies how much consideration (weight, a float value) to give a search term found in the title of an attachment.</td>
<td>Text Index Attachment Title Weight</td>
<td>FALSE</td>
<td>TRUE</td>
</tr>
<tr>
<td>text_index_auto_stop</td>
<td>boolean</td>
<td>Table</td>
<td>Both</td>
<td>Automatically identifies stop words and does not index them. Based on the threshold specified in text_index_auto_stop_threshold.</td>
<td>Text Index Auto Stop</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
<tr>
<td>Name</td>
<td>Data Type</td>
<td>Applies To</td>
<td>Applies to V3 or V4</td>
<td>Description</td>
<td>Label</td>
<td>Needs re-indexing?</td>
<td>Root Table Only</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------</td>
<td>------------</td>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------</td>
<td>-------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>text_index_auto_stop_threshold</td>
<td>int</td>
<td>Table</td>
<td>Both</td>
<td>Threshold (integer, number of occurrences) for a word to become a stop word automatically. See text_index_auto_stop.</td>
<td>Text Index Auto Stop Threshold</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
<tr>
<td>text_index_default_partial_matching_rule</td>
<td>String</td>
<td>Table</td>
<td>Both</td>
<td>String for partial matching rule configuration. Input should be based on Change the query mode of an indexed table.</td>
<td>Text Index Default Partial Matching Rule</td>
<td>FALSE</td>
<td>TRUE</td>
</tr>
<tr>
<td>text_index_default_query_mode</td>
<td>String</td>
<td>Table</td>
<td>Both</td>
<td>String for query mode configuration. Input should be based on Change the query mode of an indexed table</td>
<td>Text Index Default Query Mode</td>
<td>FALSE</td>
<td>TRUE</td>
</tr>
<tr>
<td>text_index_disable_synonym</td>
<td>boolean</td>
<td>Table</td>
<td>Both</td>
<td>TRUE disables searching on synonyms as well as the search term.</td>
<td>Text Index Disable Synonym</td>
<td>FALSE</td>
<td>TRUE</td>
</tr>
<tr>
<td>text_index_enable_idf</td>
<td>boolean</td>
<td>Table</td>
<td>V3</td>
<td>TRUE enables TF-IDF scoring.</td>
<td>Text Index Enable IDF</td>
<td>FALSE</td>
<td>TRUE</td>
</tr>
<tr>
<td>Name</td>
<td>Data Type</td>
<td>Applies To</td>
<td>Applies to V3 or V4</td>
<td>Description</td>
<td>Label</td>
<td>Needs re-indexing?</td>
<td>Root Table Only</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------</td>
<td>------------</td>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------</td>
<td>-------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>text_index_filter_junk</td>
<td>boolean</td>
<td>Table</td>
<td>Both</td>
<td>TRUE by default, FALSE disables the junk filter for a table. By default, Zing does not index or search for 2-digit numbers and single character words (unless they are Chinese or Japanese characters). Regenerate the index after disabling the junk filter. This attribute results in a larger table index. For optimal performance, do not apply it unless it is required.</td>
<td>Text Index Filter Junk</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
<tr>
<td>text_index_filter_query</td>
<td>An encodedQuery on the table</td>
<td>Table</td>
<td>Both</td>
<td>Use this attribute when you want to index the rows matching specific filter conditions. The attribute value must be an encodedQuery on the table.</td>
<td>Index Filter</td>
<td>TRUE</td>
<td>FALSE</td>
</tr>
<tr>
<td>text_index_filterable</td>
<td>boolean</td>
<td>Column</td>
<td>Both</td>
<td>If a field with this attribute set to true, is changed, the row is evaluated for re-indexing (even if the field itself is not indexable).</td>
<td>Index Filterable</td>
<td>TRUE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Name</td>
<td>Data Type</td>
<td>Applies To</td>
<td>Applies to V3 or V4</td>
<td>Description</td>
<td>Label</td>
<td>Needs re-indexing?</td>
<td>Root Table Only</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------</td>
<td>------------</td>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------</td>
<td>--------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>text_index_include_stop_word</td>
<td>boolean</td>
<td>Table</td>
<td>Both</td>
<td>if you need to index stop words in this table, set this attribute to true.</td>
<td>Text Index Include Stop Word</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
<tr>
<td>text_index_score_bm25_b</td>
<td>float</td>
<td>Table</td>
<td>V4</td>
<td>This attribute is the b parameter used in the BM25 algorithm. See text_index_score_bm25_b.</td>
<td>bm25_b</td>
<td>FALSE</td>
<td>TRUE</td>
</tr>
<tr>
<td>text_index_score_bm25_k1</td>
<td>float</td>
<td>Table</td>
<td>V4</td>
<td>This attribute is the K1 parameter used in the BM25 algorithm. See text_index_score_bm25_k1.</td>
<td>bm25_k1</td>
<td>FALSE</td>
<td>TRUE</td>
</tr>
<tr>
<td>text_index_tags</td>
<td>String</td>
<td>Table</td>
<td>Both</td>
<td>Should be set to specific String: empty/ everyone_only/ all_shared, depending on type of tags that wants to be indexed.</td>
<td>Text Index Tags</td>
<td>TRUE</td>
<td>FALSE</td>
</tr>
<tr>
<td>text_index_tokenizer_language</td>
<td>String</td>
<td>Table</td>
<td>Both</td>
<td>Put &quot;ja&quot; (without double quote) when there is need to support tokenization in Japanese.</td>
<td>Text Index Tokenizer Language</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
<tr>
<td>Name</td>
<td>Data Type</td>
<td>Applies To</td>
<td>Applies to V3 or V4</td>
<td>Description</td>
<td>Label</td>
<td>Needs re-indexing?</td>
<td>Root Table Only</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
<td>------------</td>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------</td>
<td>--------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>text_index_translations</td>
<td>Table</td>
<td>Both</td>
<td>Both</td>
<td>If present or true, forces indexes to be recalculated when translated strings are added. Requires sys-admin role to modify. Automatically set for indexed fields that are translated, and to fields that have a translation and are being indexed. The glide.i18n.force_index system property, which defaults to true, overrides this attribute.</td>
<td>Text Index Translations</td>
<td>TRUE</td>
<td>FALSE</td>
</tr>
<tr>
<td>text_search_and_or_limit</td>
<td>Table</td>
<td>Both</td>
<td>Both</td>
<td>Add table level custom attribute text_search_and_or_limit that overrides the global property.</td>
<td>Text Search And Or Limit</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>ts_language</td>
<td>String</td>
<td>Column</td>
<td>Both</td>
<td>Added to allow for text indexing of only specific languages.</td>
<td>Text Search Language</td>
<td>TRUE</td>
<td>FALSE</td>
</tr>
<tr>
<td>ts_multi_value_splitter</td>
<td>String</td>
<td>Column</td>
<td>Both</td>
<td>If one field is a multi-value field, add the splitter in the field in this attribute to spread out index positions of the values. For example, to separate multi:value, put : for this attribute.</td>
<td>Text Search Multi-value Field Splitter</td>
<td>TRUE</td>
<td>TRUE</td>
</tr>
<tr>
<td>Name</td>
<td>Data Type</td>
<td>Applies To</td>
<td>Applies to V3 or V4</td>
<td>Description</td>
<td>Label</td>
<td>Needs re-indexing?</td>
<td>Root Table Only</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------</td>
<td>------------</td>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------</td>
<td>---------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>ts_weight</td>
<td>int</td>
<td>Column</td>
<td>Both</td>
<td>Controls the relative importance of a match in the field for text search.</td>
<td>Text Search</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
</tbody>
</table>

**text_index_scorer_bm25_b**

This dictionary attribute is part of the BM25 algorithm. The attribute impacts the importance of the length of a document in search results. If this attribute is 0, the length has no bearing. In this case, a document of two words would be valued equally as a document with 1000 words. Very short documents are often weighted lower than longer documents. The default is 0.75.

**text_index_scorer_bm25_k1**

This dictionary attribute is part of the BM25 algorithm. The attribute helps determine term frequency saturation characteristics, that is, having the search term appear in a document increases the relevancy of the document, but the increase is less impactful as the numbers climb. For example, a search term occurring 10 times in a document makes it more relevant than a document that has only one occurrence. However, a document that has 100 occurrences of the search term may not be ten times more impactful than a document that has 10 occurrences. The relevance approaches a maximum effect asymptote. The higher the attribute value, the lower the maximum effect of multiple occurrences. Typical values are between 1.25 - 2.0.

**Regenerate a text index for a table**

You can regenerate a table text index when you change table stop words or display values.

Role required: admin

By default, the system maintains text indexes on a daily schedule. Typically, you only need to manually regenerate a text index when you change these values.

- You change the list of table-specific stop words.
- You change the display value of a record such as changing a user or group name.

Until you regenerate the index, text searches for old display values will still produce results and searches for the new display value will not show results.

Text indexing can be a resource-intensive task that may take a while to complete. You may notice performance degradation or incomplete search results during index generation. To estimate text indexing duration, you can view historical statistics.

*Note:* This index regeneration process purges the existing text search index for the table before it regenerates it. While it is processing, no search results are returned if you perform a text search before the regeneration is complete. An alternate method is available that does not impact use of text searches for the table while the regeneration is in process. See [Reindex a table text search without impacting returned results](#).

1. Navigate to **System Definition > Text Indexes**.
2. Open the text index for the table.

For example, select task.
The system displays the Text Index record for the table.
3. Click the **Regenerate Text Index** related link and click **OK**.
The system schedules the table for text indexing.

Reindex a table without impacting text search results

Rebuild text search indexes without adversely impacting search results. You can continue to perform text searches on a table while the index regeneration takes place.

This method does not purge the entire text search index before the rebuild takes place. It rebuilds the text search table index one record at a time, and reindexes the target table hierarchy only. For example, if you select the sc_cat_item table, only the sc_cat_item table is reindexed.

1. Navigate to System Definition > Scripts - Background.
2. In Run script box, type the following syntax for the background script, being sure to enclose both arguments in quotes as shown:

   new GlideTextIndexEvent ().indexUpdate('tableName', 'emailAddress');

   Where:
   • tableName is the name of the table you want to reindex.
   • emailAddress is the address to which an email notification should be sent when the table reindex completes. Type null for no email notification.

   For example, to regenerate the kb_knowledge table text search index, and specify that no email notification is required after the rebuild completes, create the following background script:

   new GlideTextIndexEvent ().indexUpdate('kb_knowledge', 'null');

   The script creates an event that the index handler processes so the script completes almost instantly.
3. Click the Run script button.

   The system reindexes the text search for the specified table. For large files, such as sys_metadata, reindexing can take a couple of hours, but you can still perform text searches on the table while the script is running.

Regenerate a corrupt index

Typically, a corrupt index regenerates itself. If the system does not start the regeneration process, you must issue a script command to delete the existing index and regenerate it.

1. Navigate to System Definition > Scripts - Background.
2. In Run Script box, type the syntax for the background script:

   To regenerate the task text index, the following could be used as a background script:

   ```javascript
   var indexer = new GlideLuceneTextIndexEvent();
   indexer.createIndex("task", "my_email@service-now.com");
   ```

   Change the email address to the address that receives the notification when the index is completed. The script creates an event that the index handler processes so the script completes almost instantly.
3. Click the Run script button.
4. When the scheduled job picks up the event, you can check the Component Status page and see that the index is being generated. An entry also appears in the log, as shown in the following example:

   10/28/09 15:36:19 (521) worker.1 worker.1 TextIndexGenerator: Text index generation starting for: task
As each extended table completes, it is logged:

```
10/28/09 15:37:13 (213) worker.1 worker.1 [0:00:01.462] TextIndex
generation complete for: problem, rows indexed: 11
```

After all the extended tables are completed, the Component Status page entry is updated to "completed" and a final log entry is made. The log entry shows how long the process took.

```
10/28/09 15:37:20 (794) worker.1 worker.1 TextIndexGenerator: Text index
generation complete for: task, in: 0:01:02.669
```

**Remove an index**

You can remove the index for a table if you no longer want the search engine to return results for that table. This procedure also removes the index for all tables that extend the specified table.

**Role required:** admin

1. Navigate to System Definition > Dictionary.
2. Open the dictionary entry for the table.
3. Clear the Text index check box and click Update.

The system no longer indexes or queries the table for text search results.

**Remove an index for a specific field**

You can remove the index for a specific field in a table if you no longer want the search engine to return results for that field.

**Role required:** admin

1. Navigate to System Definition > Dictionary.
2. Edit the dictionary entry for the table field.
3. In the Attributes related list, click New.
4. On the Dictionary Attribute form, fill in the fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute</td>
<td>No text index</td>
</tr>
<tr>
<td>Value</td>
<td>true</td>
</tr>
</tbody>
</table>

5. Click Submit.
6. Click Update.

The system no longer indexes or queries the table field for text search results.

**Remove an index for a child table**

You can remove the index for a child table if you no longer want the search engine to return results for that child table.

**Role required:** admin

1. Navigate to System Definition > Dictionary.
2. Edit the dictionary entry for the child table.
3. In the Attributes related list, click New.
4. On the Dictionary Attribute form, fill in the fields:
5. Click **Submit**.
6. Click **Update**.

The system no longer indexes or queries the child table for text search results.

**Change the query mode of an indexed table**

Set the query mode to specify whether searches on an indexed table must match all or only some of the search terms.

Role required: admin

To change the query mode of an indexed table, a text index must be present for the table. Make sure that text indexing is enabled for the table before changing the query mode. See Enable text indexing for a table.

Once a table is indexed, the data within the table can be searched through the global search bar. Change the query mode for the indexed table to allow global search to match all or only some of the searched terms. Enable a partial match rule to return results that partially match the searched terms.

1. Navigate to **System Definition > Text Indexes**.
2. Select the table you want to configure from the list of indexed tables.
3. Use the combo box to select a **Default query mode**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>The default query mode for a table is an AND query.</td>
</tr>
<tr>
<td>AND</td>
<td>Matches all search terms.</td>
</tr>
<tr>
<td>OR</td>
<td>Matches one or more search terms.</td>
</tr>
<tr>
<td>AND OR</td>
<td>Matches all search terms. If no results are found, matches one or more search terms.</td>
</tr>
</tbody>
</table>

4. To enable partial matching of search terms, configure the partial match rule in the **Partial Match Rule** field.

Partial match rules return results that partially match the search terms. Use a partial match rule if queries often include many keywords (if, for example, users cut and paste phrases into the global search bar).

**Partial match rules**

<table>
<thead>
<tr>
<th>Input type</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integer</td>
<td>3</td>
<td>Indicates the minimum number of search terms to be matched.</td>
</tr>
<tr>
<td>Negative integer</td>
<td>-2</td>
<td>Indicates that the number of search terms, minus this number, should be matched.</td>
</tr>
<tr>
<td>Percentage</td>
<td>75%</td>
<td>Indicates the minimum percentage of search terms to be matched. The minimum number of search terms is the number computed from the percentage rounded down.</td>
</tr>
<tr>
<td>Negative percentage</td>
<td>-25%</td>
<td>Indicates that the number of search terms, minus this percentage, should be matched. The minimum number of search terms is the number computed from the percentage rounded down and subtracted from the total number of search terms.</td>
</tr>
</tbody>
</table>
### Input type

<table>
<thead>
<tr>
<th>Input type</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Combination</td>
<td>3&lt;70%</td>
<td>A positive integer, followed by a less than symbol, followed by any of the previously mentioned input types. Indicates that if the number of search terms is equal to or less than the integer, all search terms are required. If the number of search terms is greater than the integer, the specification applies. In this example: if there are 1–3 search terms, all are required. If there are 4 or more search terms, only 70% are required.</td>
</tr>
<tr>
<td>Multiple combinations</td>
<td>3&lt;-25%, 9&lt;-5</td>
<td>Multiple conditional specifications separated by commas. In this example: if there are 1–3 search terms, all are required. If there are 4–9 search terms, all but 25% are required. If there are more than 9 search terms, all but 5 are required.</td>
</tr>
</tbody>
</table>

### Text indexing statistics and status

To view text indexing statistics and status, navigate to **System Definition > Text Indexes**.

- If text indexing is in progress, view the status of each index in the **State** field. Refresh the list to view updates.
  - Tables are indexed one at a time.
- To see how long it takes to index a specific table, view the **Last indexing duration** field for the table entry. Although each process varies based on activity and data, historical data can provide a good estimate.
- View statistics (such as the number of indexed rows, terms, and queries in the past week) in the list or on the form for a specific table.
### Text Index Status

<table>
<thead>
<tr>
<th>Text Index</th>
<th>State</th>
<th>Format</th>
<th>Indexed rows</th>
<th>Unique terms</th>
</tr>
</thead>
<tbody>
<tr>
<td>cmdh_ci_outage</td>
<td>Ready</td>
<td>v3</td>
<td>401</td>
<td>360</td>
</tr>
<tr>
<td>core_country</td>
<td>Ready</td>
<td>v3</td>
<td>231</td>
<td>1,180</td>
</tr>
<tr>
<td>kb_feedback</td>
<td>Ready</td>
<td>v3</td>
<td>17</td>
<td>320</td>
</tr>
<tr>
<td>aposec_domain_listing</td>
<td>Ready</td>
<td>v3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>cnn_location</td>
<td>Ready</td>
<td>v3</td>
<td>426</td>
<td>3,320</td>
</tr>
</tbody>
</table>
Configure tables to use the Japanese tokenizer

Improve search results in Japanese language searches by configuring individual tables to use the Japanese tokenizer.

Role required: admin

Japanese language searches use the Kuromoji Japanese tokenizer in Zing. The Japanese tokenizer attribute is active by default, but you must configure individual tables to use it and then regenerate the text index.

1. Navigate to **System Definition > Dictionary**.
2. Search for the table name.
3. In the search results, open the table, which is the list item that has an empty **Column name** and a **Type** of **Collection**.
4. Scroll down the page and click the **Attributes** tab, and then click **New**.
5. Fill in the fields on the form.

**Attributes fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute</td>
<td>Enter <strong>Text index tokenizer language.</strong></td>
</tr>
<tr>
<td>Dictionary entry</td>
<td>Defaults to the name of the table.</td>
</tr>
<tr>
<td>Value</td>
<td>Enter <code>ja</code> for the Japanese tokenizer.</td>
</tr>
</tbody>
</table>

6. Click **Submit**.

7. Regenerate a text index for a table.

**Note:** Text indexing can be a resource-intensive task that may take a while to complete. You may notice performance degradation or incomplete search results during index generation. To estimate text indexing duration, you can view historical statistics.

When the text index is generated and you go to the table you just configured, the table now uses the Japanese tokenizer.
Zing can include attachments in search results

Expand search results to include attachments from indexed tables. Display attachments for search results from the kb_knowledge table.

Sample Knowledge search showing attachments
By default, only searches of Knowledge Base records include attachments. Administrators can enable searching attachments for other tables, but doing so causes the platform to re-index the selected table, its parent table, and any children of the parent table.

**Warning:** For large tables, such as the Task table, re-indexing can take several hours and slows down the system until complete. Re-indexing is best performed during non-peak times.

The search results page only displays attachments for search results from the Knowledge [kb_knowledge] table, even if other tables have attachment search enabled.

Global search displays attachments for Knowledge search results but not for search results from other tables

Zing supports indexing and searching these attachment file types.

- .doc
- .htm
- .html

- .reg
- .txt
- .xls

- .pptx
- .potx
- .pot
Index attachments on a table

You can enable attachment indexing for a table so text searches can return matches from the record and its file attachments.

Role required: admin

By default, attachment indexing is enabled for the Knowledge Base. Enabling attachment indexing causes the platform to reindex the selected table, its parent table, and any children of the parent table. For large tables, such as the Task table, reindexing can take several hours and slows down the system until complete. Reindexing is best performed during non-peak times.

1. Open a record in the table.
2. Right-click the form header and select Configure > Dictionary.
3. On the Dictionary Entries list, open the first record.
   The first record has the record type Collection and doesn't have any entry for Column name.
4. Open the Attributes tab, and then click New.
5. On the form, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute</td>
<td>Select Attachment index.</td>
</tr>
<tr>
<td>Value</td>
<td>Enter true.</td>
</tr>
</tbody>
</table>

**Note:** The attachment indexing attribute only applies to the tables on which you explicitly add it. It does not cascade to child tables. For example, indexing attachments on the Task table does not index attachments on the Incident table. Not all file types are supported for attachment indexing. For a list of supported file types, see Zing can include attachments in search results.

6. Click Submit.
7. On the Dictionary Entry form, click the Generate Text Index related link.
8. On the confirmation window, click OK.

In the confirmation window, you can select to have the system send you an email notification after the text indexing is complete.

The indexing process begins. When it is complete, attachments can be searched on that table.

**Zing removes stop words from queries**

Remove common words from search queries that do not produce meaningful results.

Stop words are common words that are not indexed because they are not meaningful in search results. Articles, conjunctions, personal pronouns, and prepositions are examples of stop words that are not used in keyword searches. Administrators can configure stop words for all indexed tables and for specific tables.

By default, the system maintains two types of stop words.

**Types of stop words**

<table>
<thead>
<tr>
<th>Stop word type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System-wide text index stop words</td>
<td>The system always ignores system-wide text index stop words when generating text indexes. Any search for a system-wide stop word returns no search results.</td>
</tr>
<tr>
<td>Table-specific stop words</td>
<td>The system uses the table-specific Text Index record to determine whether to index the stop word or to just remove it from keyword search queries against the table.</td>
</tr>
</tbody>
</table>

By default, the system has stops words for common English words. Search administrators typically create stop words from search terms that produce too many search results such as articles, conjunctions, personal pronouns, and prepositions.
Configure a global stop word

Configure stop words that should not be indexed by the search.

1. Navigate to **System Definition > Text Index Stop Words**.
2. Add or remove stop words from the list.
3. If a message appears at the top of the list, contact Technical Support to regenerate all indexes.
   You must regenerate indexes whenever words may be missing from an index. For example, if you delete, inactivate, or change an active global stop word, the word may be missing from the index. An after business rule checks these conditions and generates the notification message when index regeneration is necessary.

Configure a table-specific stop word

You can configure stop words for a specific table.

1. Navigate to **System Definition > Text Indexes**.
2. Open the text index entry for the table.
3. Add or remove stop words from the **Index Stop Words** related list.
   For each word, select the desired **Stop mode** (Not a Stop Word (inactivates the stop word), Neither Index nor Query, or Index but do not Query).
4. If a message appears at the top of the form, click **Regenerate Text Index** and click **OK**.
   You must regenerate indexes whenever words may be missing from an index. For example, if you delete or change a stop word for which the mode was Neither Index nor Query, the word may be missing from the index.
An after business rule checks these conditions and generates the notification message when index regeneration is necessary.

**Note:** Text search uses the global list plus the table-specific list of stop words when indexing the table.

---

**Enable automatic stop words for a table**

The system can identify and generate stop words when a search term exceeds an occurrence threshold.

- Role required: admin
- Enable text indexing for the table

By default, the TS Index Stats scheduled job identifies and creates stop words for tables with text indexes on a nightly basis. Automatically adding stop words improves your search results by removing search terms that return too many search results.

1. Navigate to **System Definition > Text Indexes**.
2. Open the text index entry for the table.
3. Select the **Auto stop** check box.
4. In **Auto threshold**, enter the maximum number of occurrences a search term can have in search results. When a search term generates more search results than the threshold, the system automatically creates a stop word for the search term.

For example, to create stop words for the task table, see the blog post [Configuring auto stop words and regenerating text indexes](#) from a ServiceNow employee on the Now Community.

5. Click **Update**.

The job identifies and creates stop words for the table with a **Stop mode** value of *Index but do not Query* and inserts a **Comment** to indicate that the stop word was generated automatically.

**Zing matches derived words with stemming**

Convert any multiple-character search keyword to its stem form to find derived versions of the word.

Stemming removes a variety of common word inflections, such as plurals and past tense forms. Zing treats all words with a common stem as synonyms of the original search term. Stemming does not apply to searches involving single-character words such as Chinese and Japanese pictograms.

Zing uses the [Porter Stemming Algorithm](https://en.wikipedia.org/wiki/Porter_stemming), which is most effective for English text, but supports stemming in these languages.

- English
- French
- German

The stemming language determines how the system generates indexes of record data. The system only supports one stemming language at a time regardless of how many languages the instance supports. When you change the stemming language, the system creates any new index entries based on the new language stemming rules, but does not regenerate any existing index records. You must manually regenerate indexes for tables you want to use the new stemming language.

**Zing can expand search results with synonyms**

Expand search results to include additional search terms.

By default, Zing includes a sample synonym dictionary consisting of a list of synonym sets (synsets). Zing supports two types of synonym sets.

**Synonym set types**

<table>
<thead>
<tr>
<th>Synonym set type</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synonym list</td>
<td>A synonym list is a list of words separated by commas. When a search uses any word from the list, Zing expands the search to include all words in the list.</td>
<td>Cyber,Internet,Cybercafe</td>
</tr>
<tr>
<td>Synonym map</td>
<td>A synonym map is two word lists separated by the equal and greater than characters =&gt; . When a search uses any word from the list on the left, Zing expands the search to include all words from the list on the right. When a search uses a word from the list on the right, Zing does not expand the search to include terms from the list on the left.</td>
<td>IOT,Internet of Things=&gt;Chip,Nest thermostat,RFID,IOT</td>
</tr>
</tbody>
</table>
Search administrators can create synonym sets for search terms that produce no or low-scoring search results. See the Top Searches homepage for information about your user's search behavior.

**Search results, synonym expansion and weighting**

In search results, documents containing the original search keywords having a higher score than documents containing the search synonyms. For example, documents with the keyword IOT have a higher score than documents with the synonym Internet of Things.

- One-way synonym expansion to/from multiple terms (blork, cork => malork, elastic) works as expected. Blork and cork both expand to malork and elastic.
- Multi-level one-way expansion (blork => cork => malork) does not work transitively. Neither blork nor cork expands to malork.
- Multi-level one-way expansion split between multiple synonym set records (blork => cork) (cork => malork) does not work transitively. Only cork expands to malork, blork only expands to cork but not malork.

By default, synonyms do not use the same weight as regular search terms. Synonyms are only weighted at 10% of the default search weight. Additionally, multiple instances of a synonym in a single doc/field do not increase the search weight. The weight of synonyms is controlled by the property `glide.ts.synonym.expanded.boost`. When this property value = 1, synonyms are weighted equally to normal search terms. 0.5 = 50% weight etc.

**Enable search synonyms**

Enabling text index synonyms allows Zing to expand text searches with additional search keywords.

Role required: admin or ts_admin

By default, text searches do not use text index synonyms.

1. Navigate to System Properties > Text Search.
2. Scroll down to Enable Synonym, and click Yes.

Text searches use active synonym dictionaries to expand keyword searches.

**Create synonym dictionaries**

You can create synonym dictionaries to expand text searches with additional search keywords.

Role required: admin or ts_admin

By default, the system provides a sample synonym search dictionary called Example synonym dictionary.

1. Navigate to System Definition > Text Index Synonym Dictionaries.
2. Click New, and create a new record. See the table for field descriptions.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name for the dictionary.</td>
</tr>
<tr>
<td>Active</td>
<td>When checked the dictionary is active. The default is checked.</td>
</tr>
<tr>
<td>Global</td>
<td>When checked the dictionary is to be used on all tables that have not been individually configured. The default is checked.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the dictionary.</td>
</tr>
</tbody>
</table>
3. Add a Synonym set.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synset</td>
<td>A synonym definition, either a list or a map. Separate multiple synset words with commas. For example: medicalise, médicalisé</td>
</tr>
<tr>
<td>Active</td>
<td>When true the synonym set is used. Default is true.</td>
</tr>
<tr>
<td>Description</td>
<td>A description or notes about the synonym.</td>
</tr>
</tbody>
</table>

4. Click Submit or Update.
5. Click Publish Dictionary, under Related Links.
   The State changes from draft to Published.

Select synonym dictionaries for a table

Search administrators can specify one or more synonym dictionaries available to a particular table.

Role required: admin or ts_admin

1. Navigate to System Definition > Text Indexes.
2. Click the table for which you want to change search behavior.
   The system displays the Text index record for the table.
3. Click the Index Synonym Dictionaries tab.
4. Click New.
6. Click Submit.

Text searches on this table use the selected synonym dictionaries.

Disable synonyms for a table

By default, Zing uses all active synonym dictionaries when a user performs a text search. Search administrators can disable synonym dictionary usage on a per-table basis.

Role required: admin or ts_admin

1. Navigate to System Definition > Text Indexes.
2. Click the table for which you want to change search behavior.
   The system displays the Text index record for the table.
3. Click Disable synonym, so the check appears.
4. Click Update.

Debug synonym searches

You can view debug messages to determine if synonym searches are working as expected.

Role required: admin

1. Navigate to System Diagnostics > Session Debug > Debug Text Search.
2. Perform a search using a term in a synonym dictionary.
3. View the session debug output.
Zing displays search suggestions as users enter search terms

Display possible search query completions as users enter search terms.

To use the Search Suggestions application, activate the com.glide.search.suggestions plugin if it's not already installed. For information, see Request a plugin and Activate a plugin.

Once you enable Search Suggestions, suggestions appear automatically when users enter text into Zing search fields in the Service Portal or Now Mobile.

Automatic search suggestions

If there are any matching suggestions from the user’s own previous searches, those suggestions appear first, with a clock icon. The remaining suggestions are those suggestions coming from the searches of other users.

In the Service Portal, you can use Search Suggestions or type-ahead functionality, but not both at the same time. In Now Mobile, only Search Suggestions is available. By default, new ServiceNow instances use Search Suggestions in the Service Portal. Upgraded instances use whatever was previously enabled. You can easily enable Search Suggestions on upgraded instances. To learn more, see Enable and disable Search Suggestions in Zing.

For full details on configuration and use of the Search Suggestions application, see Search Suggestions.

Enable and disable Search Suggestions in Zing

Enable the Search Suggestions application to improve the Zing search user experience.

- ServiceNow personnel installed and activated the com.glide.search.suggestions plugin.
- Role required: admin

The Search Suggestions application is available on new instances by default. On upgraded instances, Search Suggestions is enabled for Now Mobile and disabled for Service Portal by default.

The following system properties enable and disable Search Suggestions:
• `glide.search.suggestions.enabled`: Set to `true` (default) to enable Search Suggestions in Zing, or set to `false` to disable Search Suggestions in Zing.

• `glide.service_portal.search_as_you_type_behavior`: Select `Suggestions` or `Typeahead` functionality in the Service Portal.

On new instances, the first parameter is set to `true` and the second is set to `Suggestions`. In upgraded instances, the parameters are set to whatever was previously enabled.

1. In the **Filter Navigator**, enter `sys_properties.list`.
2. To switch between Search Suggestions and type-ahead functionality in Service Portal, follow these steps.
   a) In the **Name** search column, enter `glide.service_portal.search_as_you_type_behavior`.
   b) On the System Property page, in the **Value** field, enter `Suggestions` to enable Search Suggestions, or `Typeahead` to enable type-ahead functionality. You can't enable both.

3. To turn Search Suggestions on or off globally, follow these steps.
   a) In the **Name** search column, enter `glide.search.suggestions.enabled`.
   b) In the **Value** field, double-click the value and select `true` to enable suggestions, or `false` to disable Search Suggestions globally.

---

**Set the maximum number of suggestions Zing displays**

Set the maximum number of search suggestions Zing displays when users enter search strings in Now Mobile and Service Portal.

Role required: admin

Zing displays suggestions generated by the Search Suggestions application when users enter text in a search field in a supported search application. You can control the number of suggested search strings displayed using the `sys_search_context_config_list` table for Now Mobile, and instance options for the Typeahead Search widget in Service Portal.

1. Set the maximum number of search strings displayed in Now Mobile.
   a) In the **Filter Navigator**, enter `sys_search_context_config_list`.

---

© 2021 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
b) In the Search Context Configurations list, in the row where Application ID equals ServiceNow Mobile Request Native Application, double-click the number in the Suggestions limit column.

c) Update the number and click the green check mark.

2. Set the maximum number of search strings displayed for Knowledge Base searches.
   a) Navigate to Service Portal: https://<instance name>/service-now.com/sp.
   b) Click the Knowledge Base link.
   c) Place your cursor in the search field.
   d) While holding down the Control key, press the left mouse key.
      A context menu appears.
   e) Click Widget Options Schema.
   f) Scroll down to the section where Label is Limit, enter the maximum number of search suggestions to display in the Default value field, then click Save at the bottom of the form.

   Note: You can limit the number of search suggestions on any form that uses the Typeahead Search widget. For example, the System Status tab also uses the typeahead widget but the Catalog tab does not. For more information, see Typeahead Search widget

Installed with Zing

Several types of components are installed with Zing.

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text Index [ts_index_name]</td>
<td>Stores the tables the system indexes.</td>
</tr>
<tr>
<td>Index Stop Word [ts_index_stop]</td>
<td>Stores the stop words for a specific table.</td>
</tr>
<tr>
<td>Stop Word [ts_stop]</td>
<td>Stores the global stop words.</td>
</tr>
<tr>
<td>Text Search Groups [ts_group]</td>
<td>Stores search groups for global text search.</td>
</tr>
</tbody>
</table>

- ts_attachment
- ts_chain_summary
- ts_chain
- ts_deleted_doc
- ts_document
- ts_index_stats
- ts_phrase
- ts_search_stats
- ts_search_summary
- ts_word_roots
- ts_word

System tables that support Zing. Extending or modifying these tables is not recommended.
## Business rules installed with Zing

<table>
<thead>
<tr>
<th>Business Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text Search Property Change Rationally</td>
<td>Ensures that valid values are entered for Zing text search properties.</td>
</tr>
<tr>
<td>Text Index Stop Reminder</td>
<td>Warns the user of stop word changes that require the index to be rebuilt (table-specific). The warning is issued if record is deleted that had a stop mode “neither index nor query”, if record's stop mode is updated to something else and was “neither index nor query”, and if record's word is updated to something else and stop mode is &quot;neither index nor query&quot;.</td>
</tr>
<tr>
<td>Stop Word Reminder</td>
<td>Warns the user of stop word changes that require the index to be rebuilt (global). The warning is issued if record is deleted and it was active, if record is inactivated, and if record’s word is changed and was active.</td>
</tr>
</tbody>
</table>

## Scheduled jobs installed with Zing

<table>
<thead>
<tr>
<th>Scheduled job</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TS Search Stats</td>
<td>Compiles type-ahead suggestions each night. See Update A Type-Ahead Suggestion.</td>
</tr>
<tr>
<td>TS Index Stats</td>
<td>Collects statistics and performs maintenance for text search and indexing. Runs nightly.</td>
</tr>
<tr>
<td>text index events process</td>
<td>Collects statistics and performs maintenance for text search and indexing. Runs every 30 seconds.</td>
</tr>
<tr>
<td>TS Search Summary</td>
<td>Compiles top search statistics each hour. See Update a top search statistic.</td>
</tr>
<tr>
<td>TS Chain Summary</td>
<td>Compiles search chain statistics each hour.</td>
</tr>
</tbody>
</table>

## UI action installed with Zing

<table>
<thead>
<tr>
<th>UI action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regenerate Text Index</td>
<td>Displays the Regenerate Text Index link on Text Index forms.</td>
</tr>
</tbody>
</table>

## Homepage installed with Zing

<table>
<thead>
<tr>
<th>Homepage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Searches homepage</td>
<td>Displays the most popular searches over the past hour, day, week, or month.</td>
</tr>
</tbody>
</table>
AI Search

The application provides a modern consumer-grade search engine for , , and . Intelligent query features enable users to quickly find the answers they need.

Get started

Troubleshoot and get help

• Ask or answer questions about AI Search in the Now Community
• Search the Known Error Portal for known error articles
• Contact Customer Service and Support

Extend AI Search with apps from the ServiceNow® Store

• Analyze search query traffic trends, review indexed record counts and configuration settings, and preview search query results with Advanced Management Tools.

Exploring AI Search

Learn about AI Search features that enable you to provide consumer-grade search experiences for your users.

Index searchable content from Now Platform tables

Make record content searchable by adding it to the AI Search index.

Define an indexed source for each Now Platform table that you want to index records from. Search administrators can configure settings for each indexed source:

• Enable indexing for child tables of the source table.
• Configure indexing of source record tags, attachments, translated fields, and referenced fields.
• Map source table fields to AI Search index fields for ease of search.
The base system includes indexed sources for Knowledge Base articles, CMDB Catalog Items, and user records. You can create indexed sources to index records from almost any other Now Platform table.

Search administrators define indexed sources and use them to index content. To learn more about indexed sources, see Indexed sources.

Control access to searchable content using search sources

A search source defines a subset of indexed content that users can search using a search profile. Create search sources by applying filter conditions to content from indexed sources.

Search administrators link search sources to search profiles, enabling precise control of the content that users can search. For details on creating search sources, see Search sources.

Define search experience settings in search profiles

Search profiles define search sources and settings for linguistic search query features. Each search profile represents an individual search experience that you want to offer users in a supported Now Platform.

Each search profile can include the following settings:

- One or more search sources defining content that users can search using the profile.
- Dictionaries of synonyms, stop words, and typo handling auto-correction terms applied to searches using the profile.
- Genius Result configurations applied to searches using the profile.
- Result improvement rules applied to searches using the profile.

Search administrators create search profiles, link search sources to them, configure their settings, and publish them. For information on creating, configuring, and publishing search profiles, see Search profiles.

Enable AI Search in supported Now Platform applications

Provide multiple search entry points across your organization by enabling AI Search as the search engine for , , and .

Search administrators define search application configurations for Now Platform applications. Each configuration links to a search profile defining the search experience for the application. Administrators can configure the application's behavior in the following ways:

- Enable or disable typo handling auto-correction for search queries.
- Configure navigation tab and facet filters to enable users to refine search results.
- Limit the maximum number of search suggestions and Genius Result cards the application can display for a search.
- Limit the number of search results the application displays on each result page.
- Enable or disable highlighting of search query terms in the application's search results.

To learn more about configuring and enabling AI Search in supported Now Platform applications, see Search application configurations and Enabling and configuring AI Search in Now Platform applications.

Provide users with powerful and flexible search

AI Search includes search features that help users find the answers they need.

**Powerful query language**

Query for indexed terms and phrases. Control query logic with Boolean operators. Match a range of indexed terms using wildcard operators.

For a complete guide to supported query language syntax and operators, see AI Search query language.

**Auto-complete search queries**
Display suggestions in the input field as users compose their searches. Suggestions include recent and popular search queries and results as well as entries from the user's personal search history.

Auto-complete suggestions are linguistic features that search administrators configure in search application configurations. For more information on auto-complete suggestion type settings, see Configure an auto-complete suggestion type in an AI Search application configuration.

**Language-sensitive lemma and Unicode normalization of search query terms**

Support natural language search by expanding search query terms to match alternate inflections and forms.

Lemma and Unicode normalization are linguistic features that do not require configuration. For more details on normalization behavior, see Lemma and Unicode normalization.

**Expand search query terms using configurable synonyms**

Improve search recall by configuring language-specific dictionaries of terms with equivalent meanings or usage. When a search query includes any of these terms, AI Search expands it to include all equivalent terms, providing users with a more natural search experience.

Synonyms are linguistic features that search administrators configure in search profiles. For details on synonyms and synonym dictionaries, see Synonyms.

**Remove excessively frequent search terms using configurable stop words**

Increase search precision by configuring language-specific dictionaries of frequently appearing terms that dilute search relevancy. AI Search removes these stop words from user search queries to exclude irrelevant results.

Stop words are linguistic features that search administrators configure in search profiles. For details on stop words and stop word dictionaries, see Stop words.

**Auto-correct typos in search query terms**

Automatically replace misspelled search query terms with spellings found in indexed content. Typo corrections are displayed above search results. Users can always choose to repeat the search with their original query terms.

Typo handling auto-correction is a linguistic feature that search administrators configure in search profiles. For details on controlling the set of available auto-correction terms, see Typo handling.

**Enable search result refinement filters**

AI Search enables users to refine searches by filtering their results. Use navigation tabs to filter results by source, or select facets to apply filters dynamically generated from the result set.

**Filter results by source using navigation tabs**

Display pre-defined categories that users can select to immediately exclude unwanted search results.

Search administrators configure navigation tabs in search application configurations. For details on available settings, see Configure navigation tabs in an AI Search application configuration.

**Filter results dynamically using facets**

Display field value-based filter selections generated dynamically from the search query's result set. Users can select multiple facet values to narrow their area of focus. Facets only display when they produce results, so users never need to worry about dead ends.

Search administrators define facets in search application configurations. For details on creating and configuring facets, see Create a facet in an AI Search application configuration.
Display relevant and actionable search results

AI Search provides users with clear answers for their search queries.

Display the most relevant results first with machine learning relevancy

AI Search orders search results in decreasing order of relevancy. Machine learning automatically tunes and improves search result relevancy scoring based on aggregated signal data from user interactions with search.

Machine learning relevancy is automatically enabled and not configurable. For more details on automatic relevancy score tuning, see Machine learning relevancy in AI Search.

Display the best answers as actionable Genius Result cards

Configure optional Genius Results to analyze search query intent and put the best answers first. Search users can read a Knowledge article, view a user's profile or organization chart, or request a Catalog Item directly from a Genius Result answer card.

Search administrators can link Genius Results to search profiles, modify their settings, and create new configurations. For details on Genius Results configurations, see Genius Results.

Boost, block, or promote search results

Define result improvement rules with configurable trigger conditions. A rule can boost search result relevancy based on the search query or user context, or can block or promote specific results for a particular search query.

Search administrators define result improvement rules in search profiles. For details on creating rules and configuring their boost, block, or promote actions, see Result improvement rules.

Hit highlighting

AI Search highlights search query terms that appear in search results. This highlighting enables users to see which query terms contributed to record matches.

Search administrators configure hit highlighting in search application configurations. For details on controlling this setting, see Enable or disable hit-highlighting for an AI Search application.

Content security in AI Search

When indexing records, AI Search preserves their Now Platform security features. At query time, AI Search filters search query results and displays only records that the user can access.

For more information on how AI Search handles security features for Now Platform table records, see Content security in AI Search.

Internationalization support

Index and search for content in any language supported by the Now Platform. Configure linguistic search features in English, French Canada, French, German, Japanese, and Spanish.

For more details on language support in AI Search indexing, search, and linguistic query features, see Internationalization support for AI Search.

Deflect incidents in Service Portal with the AI Search Assist widget

Improve incident deflection for Service Portal users by displaying the most relevant search results within a record producer.

AI Search Assist can help an agent or user find the most relevant items in a search on your portal. For example:

- An agent, working on an Incident record, can use AI Search Assist to find and attach knowledge articles, order a catalog item on behalf of the caller, or search for an article and link it to a related incident or problem.
• A user, creating an Incident via the Service Portal, can see related Catalog Items that the user can order. The user can also view related knowledge articles to help them resolve the issue on their own without involving the service desk operators.

AI Search Assist helps with incident deflection for the following areas:
• Incident record producers: Deflect incidents by helping end users resolve issues before they raise an incident.
• Incident forms: Help service desk staff resolve incidents quickly by providing relevant knowledge.
• Incident email notifications: Help end users resolve their incidents themselves without requiring manual intervention from service desk staff.

To learn more about configuring and using the AI Search Assist widget in Service Portal, see AI Search Assist.

Configuring AI Search
Plan and configure your AI Search implementation.

Configuration overview

<table>
<thead>
<tr>
<th>Configuration stage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign roles to AI Search administrators</td>
<td>Assign the ais_admin role to users who need to create, read, update, and delete content indexing and search settings for AI Search. Assign the search_application_admin to users who need to create, read, update, and delete search application configurations.</td>
</tr>
<tr>
<td>Define indexed sources</td>
<td>Create and configure an indexed source for each Now Platform table that has content you want to make searchable. Index source tables to add their searchable content to the AI Search index. The base system includes pre-configured indexed sources for the Catalog Item, Knowledge, and User tables.</td>
</tr>
<tr>
<td>Define search sources</td>
<td>Apply filter conditions to indexed sources to define search sources that users can access in your search experiences. The base system includes pre-configured search sources that reference the default indexed sources.</td>
</tr>
<tr>
<td>Define search profiles</td>
<td>Create a search profile for each distinct search experience that you want to offer in search applications. Specify the data that users can search by linking search sources to the search profile. Control search behavior by configuring synonyms, stop words, typo handling settings, Genius Results, and result improvement rules. The base system includes pre-configured search profiles for use with Service Portal, Now Mobile, and the AI Search Assist Service Portal widget.</td>
</tr>
</tbody>
</table>
### Configuration stage

<table>
<thead>
<tr>
<th>Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Define search application configurations</strong></td>
<td>Create a configuration for each Now Platform application that supports AI Search. Select a search profile for the application to use. Configure application-specific search settings. The base system includes pre-configured search application configurations for Service Portal, Virtual Agent, and the AI Search Assist Service Portal widget.</td>
</tr>
<tr>
<td><strong>Enable and configure AI Search in Now Platform applications</strong></td>
<td>Specify AI Search as the search engine in supported Now Platform applications. Select a search application configuration for each application to use and configure available search UX settings.</td>
</tr>
</tbody>
</table>

### Using guided setup to implement AI Search

Guided setup provides a sequence of tasks that help you configure AI Search on your ServiceNow instance. To open AI Search guided setup, navigate to **AI Search > Guided Setup**.

For more information about using the guided setup interface, see Using guided setup.

### Assign roles to AI Search administrators

Grant users the ais_admin and search_application_admin roles so they can configure and manage settings for AI Search and search applications.

Role required: admin

Users with the following roles can access and configure settings for the AI Search application.
<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
</table>
| administrator [ais_admin]                 | Manages configuration settings for the application, including the following:  
  • Creates, reads, updates, and deletes indexed sources  
  • Creates, reads, updates, and deletes search sources  
  • Creates and deletes mappings between search sources and search profiles  
  • Creates, reads, updates, and deletes search profiles  
  • Creates, reads, updates, and deletes synonym and stop word dictionaries  
  • Creates and deletes mappings between dictionaries and search profiles  
  • Reads and updates typo handling auto-correction dictionaries linked to search profiles  
  • Creates, reads, updates, and deletes Genius Result configurations  
  • Creates and deletes mappings between Genius Result configurations and search profiles  
  • Creates, reads, updates, and deletes result improvement rules  
  • Creates and deletes mappings between result improvement rules and search profiles  
  This role is included in the Search application administrator [search_application_admin] role.                                                                                                                                                                                                                     |
| Search application administrator [search_application_admin] | Creates, reads, updates, and deletes search application configurations.  
   This role includes the ais_admin and personalize_dictionary roles.                                                                                                                                                                                                                                                                                                                                                               |

Assign these roles to users and groups to enable them as search administrators for AI Search.

- Assign a role to a user
- Assign a role to a group

**Indexed sources**

Indexed sources enable AI Search to retrieve records from Now Platform tables. Index a source table's records to make their content searchable in AI Search.

Each indexed source includes a unique name and a reference to a Now Platform table. AI Search extracts searchable content from records in this table, and in any of its child tables that you configure for indexing.

When you define a new indexed source, automatically begins indexing changes made to records in the selected source table and its specified child tables. It doesn't index content from existing records in these tables until you perform a full table index.

**Note:** excludes some tables from indexing. You cannot define these excluded tables or their derived tables as indexed sources. For a list of excluded tables, see Now Platform tables excluded from AI Search indexing.

You can configure attributes and field settings for an indexed source to control indexing behavior for source records.
Create an indexed source
Define an indexed source to make content from records on a Now Platform table searchable using AI Search.

Role required: ais_admin

1. Navigate to **AI Search > AI Search Index > Indexed Sources**.
2. Click **New**.
3. On the form, fill in the fields.

### AI Search Indexed Sources form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name for the indexed source.</td>
</tr>
<tr>
<td>Source</td>
<td>The Now Platform table to index.</td>
</tr>
<tr>
<td>Active</td>
<td>Option to activate the indexed source. Only active indexed sources can index content from Now Platform tables.</td>
</tr>
<tr>
<td>Application</td>
<td>Application scope for the indexed source. This field is automatically set.</td>
</tr>
</tbody>
</table>

**Note:** excludes some tables from indexing. You cannot define these excluded tables or their derived tables as indexed sources. For a list of excluded tables, see Now Platform tables excluded from AI Search indexing.

4. Click **Submit**.
   The new indexed source appears in the AI Search Indexed Sources list with the **State** set to **New**. If the new indexed source requires manual indexing, an informational message and an alert triangle icon (⚠️) appear.

5. Optional: To configure indexing for child tables of the selected source table, edit the new indexed source and follow these steps for each child table:
   a) In the Child Tables related list, click **New**.
   b) On the form, fill in the fields.

### Child Table form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indexed Source</td>
<td>Reference to the indexed source. This field is automatically set.</td>
</tr>
<tr>
<td>Table</td>
<td>Label and name for the child table that you want to enable content indexing for. You can only select from tables that extend the indexed source table.</td>
</tr>
<tr>
<td>Active</td>
<td>Option to activate indexing for the child table.</td>
</tr>
<tr>
<td>Application</td>
<td>Application scope for the child table indexing configuration. This field is automatically set.</td>
</tr>
</tbody>
</table>
c) Click **Submit**.
   The new child table appears in the Child Tables related list.

Perform a full table reindex for the indexed source to make content from existing records searchable. For details on this procedure, see **Perform a full table index or reindex for a single indexed source.**

*Indexed source attributes*

An indexed source attribute defines indexing behavior for all records from an indexed source.

Examples of how you might use indexed source attributes include the following.

- Define a filter to limit the set of records indexed from the source table
- Modify default indexing behavior for attachments or tags found on source table records
- Specify whether to index translated fields from source table records

Indexed source attributes appear in the indexed source's Advanced Configuration related list.

Create an indexed source attribute

Define an indexed source attribute to configure the AI Search content indexing behavior for all records on a source table.

Role required: ais_admin

For details on available indexed source attributes and values, see **List of AI Search indexed source attributes.**

1. Navigate to **AI Search > AI Search Index > Indexed Sources.**
2. Edit the indexed source that you want to define an attribute for.
3. In the Advanced Configuration related list, click **New.**
4. On the form, fill in the fields.

**Indexed Source Attribute form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indexed Source</td>
<td>Indexed source the attribute applies to.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Attribute to set for all records indexed from the selected source table.</td>
</tr>
<tr>
<td>Application</td>
<td>Application scope for the indexed source attribute. This field is automatically set.</td>
</tr>
<tr>
<td>Source</td>
<td>Specific table from the indexed source that the attribute applies to.</td>
</tr>
<tr>
<td>Value</td>
<td>Value for the specified attribute.</td>
</tr>
</tbody>
</table>

5. Click **Submit**.

The new indexed source attribute appears in the Advanced Configuration related list.

To make the new indexed source attribute take effect, perform a full table reindex for the indexed source. For details on this procedure, see **Perform a full table index or reindex for a single indexed source.**

Enable indexing of tags for an indexed source

Configure an indexed source attribute to enable indexing of content from tags found on records from an indexed source.

Role required: ais_admin

By default, AI Search indexing ignores tags from source records. You can enable indexing of tags for all records from an indexed source. Choose whether you want to index all shared and globally visible tags or just globally visible tags. Private tags are never indexed.
For more general instructions on defining indexed source attributes, see Create an indexed source attribute.

1. Navigate to **AI Search > AI Search Index > Indexed Sources**.
2. Edit the indexed source that you want to enable tag indexing for.
3. In the Advanced Configuration related list, click **New**.
4. On the form, fill in the fields.
   a) In the **Attribute** field, enter `index_tags`.
   b) In the **Value** field, enter one of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>everyone_only</td>
<td>Only tags shared with everyone are indexed.</td>
</tr>
<tr>
<td>all_shared</td>
<td>All shared tags (Everyone, Groups and Users) are indexed.</td>
</tr>
</tbody>
</table>

5. Click **Submit**.

The new **index_tags** indexed source attribute appears in the Advanced Configuration related list.

To make the new **index_tags** attribute take effect, perform a full table reindex for the indexed source. For details on this procedure, see Perform a full table index or reindex for a single indexed source.

List of AI Search indexed source attributes

You can adjust indexing behavior for an AI Search indexed source by configuring indexed source attributes and values.

For instructions on defining AI Search indexed source attributes, see Create an indexed source attribute.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter</td>
<td>Specify a filter condition that applies on the indexed source table and all of its child tables configured for indexing. Indexing ignores source records that do not pass this filter condition.</td>
</tr>
</tbody>
</table>
| index_attachments | Control indexing behavior for attachments from indexed records. Supported values:  
|                 | • **false**: Disable indexing of attachments for this table.  
|                 | • **true**: Enable indexing of attachments for this table. |
| index_tags     | Control indexing behavior for tags from indexed records. Supported values:  
|                 | • **all_shared**: Index shared tags and globally visible tags.  
|                 | • **everyone_only**: Only index globally visible tags.  
|                 | • **none**: Disable indexing of tags. |

**Note:** Search results display indexed tags based on the visibility of the result record instead of the visibility of the tag.
### Field settings

A field setting controls indexing behavior for a specified field (column) on all records from an indexed source.

Examples of how you might use field settings include the following:

- Disable text indexing for a specified field found on source table records
- Modify mappings between a specified source table and an AI Search field
- Add a field to the index by dot-walking from reference fields on source table records

Field settings appear in the indexed source's Field Settings & Mapping related list.

**Create a field setting for an indexed source**

Define an indexed source field setting to configure AI Search content indexing behavior for a specific field on source table records.

Role required: ais_admin

For details on available field settings and values, see [List of AI Search indexed source field settings](#).

1. Navigate to **AI Search > AI Search Index > Indexed Sources**.
2. Edit the indexed source that you want to define a field setting for.
3. In the Field Settings & Mapping related list, click **New**.
4. On the form, fill in the fields.

5. **Click Submit.**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indexed Source</td>
<td>Indexed source that the field setting applies to.</td>
</tr>
<tr>
<td>Source</td>
<td>Specific table from the indexed source that the field setting applies to.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Field setting to apply for the selected field on all records indexed from the selected source table.</td>
</tr>
<tr>
<td>Application</td>
<td>Application scope for the field setting. This field is automatically set.</td>
</tr>
<tr>
<td>Field</td>
<td>Record field that the field setting operates on.</td>
</tr>
<tr>
<td>Value</td>
<td>Value for the specified field setting.</td>
</tr>
</tbody>
</table>
The new field setting appears in the Field Settings & Mapping related list.

To make the new field setting take effect, perform a full table reindex for the indexed source. For details on this procedure, see Perform a full table index or reindex for a single indexed source.

List of AI Search indexed source field settings

You can adjust indexing behavior for source record fields in an AI Search indexed source by configuring field setting attributes and values.

For more information on creating field settings, see Create a field setting for an indexed source.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot_walk_fields</td>
<td>Index searchable content from fields on the table referenced by the selected field.</td>
</tr>
<tr>
<td></td>
<td>• Type: String</td>
</tr>
<tr>
<td></td>
<td>• Value: Comma-separated list of referenced table fields to index</td>
</tr>
<tr>
<td>map_to</td>
<td>Map display values from the selected field to an AI Search index field for records from the indexed source.</td>
</tr>
<tr>
<td></td>
<td>• Type: String</td>
</tr>
<tr>
<td></td>
<td>• Value: Name of the AI Search field that you want to map the selected field's display values to. For details on AI Search index fields, see AI Search index fields.</td>
</tr>
<tr>
<td>map_to_raw</td>
<td>Map native database values from the selected field to an AI Search index field for records from the indexed source.</td>
</tr>
<tr>
<td></td>
<td>• Type: String</td>
</tr>
<tr>
<td></td>
<td>• Value: Name of the AI Search field that you want to map the selected field's native database values to. For details on AI Search index fields, see AI Search index fields.</td>
</tr>
<tr>
<td>no_text_index</td>
<td>Option to disable indexing of searchable content from the selected field on records from the indexed source.</td>
</tr>
<tr>
<td></td>
<td>Supported values:</td>
</tr>
<tr>
<td></td>
<td>• true: Disable searchable content indexing for the selected field. Search and filters cannot match the field's value.</td>
</tr>
<tr>
<td></td>
<td>• false: Enable searchable content indexing for the selected field. Search and filters can match the field's value.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>not_searchable</td>
<td>Option to disable search matching for content indexed from the selected field.</td>
</tr>
<tr>
<td></td>
<td>Supported values:</td>
</tr>
<tr>
<td></td>
<td>• <strong>true</strong>: Disable search matching for content indexed from the selected field. Search cannot match the field's value. Filters (such as for content security, navigation tabs, and facets) can still match the field's value.</td>
</tr>
<tr>
<td></td>
<td>• <strong>false</strong>: Enable search matching for content indexed from the selected field. Search and filters can match the field's value.</td>
</tr>
</tbody>
</table>

This example shows how to map `short_description` display field values from an indexed source's records to the AI Search `title` field.

**Indexing content from indexed sources**

AI Search indexes records on indexed source tables to make their content searchable.

When you define a new indexed source, automatically begins indexing changes made to records in the selected source table and its specified child tables. It doesn't index content from existing records in these tables until you perform a full table index.

**Indexing content from referenced tables**

When an indexed source table includes a reference field, AI Search defaults to indexing values for the reference field but not for other fields on the referenced record.

You can configure a `dot_walk_fields` field setting to index additional fields from referenced tables. For more information on field settings, see Field settings.
Indexing content from source record attachments

AI Search indexes searchable content and metadata (such as file size and date) for attachments found on source table records. Indexing supports the following attachment file formats:

• Hypertext Markup Language (.html, .htm)
• Excel (.xls, .xlsx)
• PowerPoint (.pot, .potx, .ppt, .pptm, .pptx)
• Word (.doc, .docx, .dot, .dotx)
• Plain Text (.txt)
• Portable Document Format (.pdf)

AI Search provides limited support for encrypted record attachments:

• When indexing an encrypted attachment, AI Search extracts metadata such as file size and date, but doesn't extract searchable content.
• The encrypted attachment's MIME type is detected as application/octet-stream.
• No feedback for the encrypted attachment appears in ingestion log messages.

Indexing content from source record tags

AI Search can index tags found on source table records. Search results display indexed tags based on the visibility of the result record instead of the visibility of the tag.

By default, indexing ignores tags from source records. You can enable indexing of tags for each indexed source. Choose whether you want to index all shared and globally visible tags or just globally visible tags.

For details on enabling tag indexing for an indexed source, see Enable indexing of tags for an indexed source.

Reindexing content

You must perform a full table reindex for an indexed source under the following circumstances:

• After you add, modify, or delete an indexed source attribute or a field setting for the indexed source.
• If you want to update indexed values for fields on records referenced from source table records.

Perform a full table index or reindex for a single indexed source

Make content from an indexed source searchable by performing a full table index. This procedure indexes existing records from the source table and any child tables configured for indexing. You can manually reindex content from an indexed source by repeating these steps.

Role required: ais_admin

When you define a new indexed source, automatically begins indexing changes made to records in the selected source table and its specified child tables. It doesn't index content from existing records in these tables until you perform a full table index.

Follow these steps to index searchable content from existing records in an indexed source. Use the same steps to manually reindex existing content for an indexed source that has already been indexed.

If an indexed source contains unindexed records, the Indexed Sources list displays an informational message and marks the new source with an alert triangle icon (⚠️). A similar informational message appears on the Indexed Source form. Make sure to perform a full table index for each indexed source that displays the alert triangle icon.

1. Navigate to **AI Search > AI Search Index > Indexed Sources.**
2. Edit the indexed source with content that you want to make searchable.
3. Click **Index All Tables**.
   The Indexed Source History page appears. A message reports that AI Search has queued an indexing task for the indexed source.
4. Optional: Refresh the Indexed Source History form page to monitor the progress of the indexing task.
   When the task completes, the **Ingestion State** field shows **indexed**.
5. To return to the list of indexed sources, click the back icon ( ).

AI Search indexes content from existing records in the indexed source. Indexing continues on a scheduled basis. You don't need to repeat this task for the indexed source unless you want to reindex its content before the next scheduled indexing run.

Define search sources to make searchable content from the indexed source available in user search experiences. For details on creating search sources, see **Create a search source**.

Role required: ais_admin

When you define a new indexed source, **automatically begins indexing changes made to records in the selected source table and its specified child tables. It doesn't index content from existing records in these tables until you perform a full table index.**

Follow these steps to index searchable content from existing records in indexed sources. Use the same steps to manually reindex content for indexed sources that have already been indexed.

If an indexed source contains unindexed records, the Indexed Sources list displays an informational message and marks the new source with an alert triangle icon ( ). A similar informational message appears on the Indexed Source form. Make sure to perform a full table index for each indexed source that displays the alert triangle icon.

1. Navigate to **AI Search > AI Search Index > Indexed Sources**.
2. Select the action options next to the indexed sources with content that you want to make searchable. To select all indexed sources on the page, follow the instructions for your list version in **Perform actions on selected items in a list**.
3. In the Actions on selected rows menu at the bottom of the list, click **Index All Tables**.
   The Indexed Source History page for the last selected index appears. A message reports that AI Search has queued an indexing task for the indexed source.
4. Optional: Refresh the Indexed Source History form page to monitor the progress of the indexing task.
   When the task completes, the **Ingestion State** field shows **indexed**.
5. To return to the list of indexed sources, click the back icon ( ).

AI Search indexes content from existing records in the indexed sources. Indexing continues on a scheduled basis. You don't need to repeat this task for the indexed sources unless you want to reindex their content before the next scheduled indexing run.

Define search sources to make searchable content from indexed sources available in user search experiences. For details on creating search sources, see **Create a search source**.
Search sources

Define search sources to make your searchable content available in search experiences. Choose an indexed source and configure optional filter conditions to limit the content that users can search.

Search source structure

A search source includes two elements:

- A reference to an indexed source. By default, search queries using the search source can return all records from the referenced indexed source. For more information on indexed sources, see Indexed sources.
- An optional set of filter conditions applied to the indexed source's records. Indexed source records must pass all of these filter conditions to be returned as search results for queries using the search source. For more information on filter conditions, see Filters.

You can define multiple search sources that reference the same indexed source, specifying distinct filter conditions for each.

Linking search sources to search profiles

To make your search source's content available to users, link it to one or more search profiles. You can link multiple search sources to a single search profile.

For more information, see Link a search source to a search profile.

Viewing search sources

You can view or edit search sources from any of the following locations:

- To view all defined search sources, navigate to AI Search > Search Experience > Search Sources.
- To view search sources that reference a particular indexed source, navigate to AI Search > Al Search Index > Indexed Sources. Edit the indexed source and select its Search Source Mappings related list.
- To view search sources linked to a particular search profile, navigate to AI Search > Search Experience > Search Profiles. Edit the search profile and select its Search Sources related list.

Create a search source

Make searchable content from an indexed source available in user search experiences by defining a search source.

You must have an indexed source defined. For more details on setting up indexed sources, see Create an indexed source.

Role required: ais_admin

Define at least one search source for each of your indexed sources. You can define multiple search sources that reference the same indexed source, specifying distinct filter conditions for each.

1. Navigate to AI Search > Al Search Index > Indexed Sources.
2. In the Search Source Mappings related list, click New.
3. On the form, fill in the fields.

**AI Search Source form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indexed source</td>
<td>Reference to an indexed source. For more details on indexed sources, see Indexed sources.</td>
</tr>
<tr>
<td>Conditions</td>
<td>Set of filter conditions that documents from the indexed source must meet to be included in the search source. For more details on filter conditions, see Filters.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

The new search source appears in the Search Sources related list.

**Preview matching records for a search source**

View the Now Platform table records that match a search source’s indexed source table and filter conditions.

Role required: ais_admin

1. Navigate to **AI Search > Search Experience > Search Sources**.
2. Edit the search source that you want to preview matching records for.
3. On the Search Source form, click the **preview** link in the informational message that reports the number of matching records.

The Now Platform table specified in the search source's indexed source appears, with filter conditions applied to match conditions from the search source. This filtered view displays all records that are searchable through the search source.

**Note:** Preview uses the saved conditions from the search source. If you change a search source's conditions, preview does not reflect your changes until you save them.

**Search profiles**

AI Search stores search experience settings in search profiles. Define a search profile for each unique search experience that you want to offer users in a Now Platform application. Create and populate synonym and stop word dictionaries. Configure typo handling dictionary settings. Define Genius Results and result improvement rules.

The following table describes the search experience settings that you can configure in a search profile.

**Search profile settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search sources</td>
<td>Link one or more search sources to a search profile. Search sources give administrators precise control over the searchable content available to users.</td>
</tr>
<tr>
<td>Synonyms</td>
<td>Define language-specific dictionaries of terms that AI Search treats as equivalent in search queries. Synonyms improve search recall and provide a more natural search experience for users.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Stop words</td>
<td>Define language-specific dictionaries of common terms for AI Search to remove from search queries. Stop words improve search precision and result relevancy by discarding irrelevant matches.</td>
</tr>
<tr>
<td>Typo handling</td>
<td>Configure settings for derivation of auto-correction terms from search source indexed content. AI Search replaces misspelled search query terms with auto-correction terms.</td>
</tr>
<tr>
<td>Genius Results</td>
<td>Analyze search query intent and display the best answers as Genius Result answer cards. Genius Results enable users to act directly on their search results.</td>
</tr>
<tr>
<td>Result improvement rules</td>
<td>Define rules with configurable triggers to modify search results for specific search queries. Result improvement rules enable administrators to boost, block, or promote records in a search query's result set.</td>
</tr>
</tbody>
</table>

**Publishing search profile settings**

To make a search profile's settings active in search queries, you must publish it. Publishing propagates the following settings to search application configurations that reference the search profile:

- The set of synonym and stop word dictionaries linked to the search profile
- Settings, blocked terms, and derived auto-correction terms for typo handling dictionaries linked to the search profile
- Result improvement rules and actions defined in the search profile

A search profile can have one of these states:

- **New**: The search profile has never been published.
- **Draft**: The search profile is saved with unpublished changes.
- **Published**: The search profile is saved with all changes published.

In the **Al Search > Search Experience > Search Profiles** list, search profiles with the **New** state display an alert triangle icon (⚠️). An informational message notifies you to publish these search profiles.

*Create a search profile*

Create a new search profile to store search experience settings for a search application.

Role required: ais_admin

1. Navigate to **Al Search > Search Experience > Search Profiles**.
2. Click **New**.
3. On the form, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>Unique label for the search profile.</td>
</tr>
<tr>
<td>Description</td>
<td>Text description for the search profile.</td>
</tr>
<tr>
<td>Application</td>
<td>Application scope for the search profile. This field is automatically set.</td>
</tr>
<tr>
<td>Updated</td>
<td>Last update date for the search profile. This field is automatically set.</td>
</tr>
<tr>
<td>Updated by</td>
<td>User who most recently updated the search profile. This field is automatically set.</td>
</tr>
<tr>
<td>Active</td>
<td>Option to activate the search profile.</td>
</tr>
<tr>
<td>State</td>
<td>State of the search profile.</td>
</tr>
<tr>
<td></td>
<td>• <strong>New</strong>: The search profile has never been published.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Draft</strong>: The search profile is saved with unpublished changes.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Published</strong>: The search profile is saved with all changes published.</td>
</tr>
</tbody>
</table>

4. Click **Submit**. The new search profile appears in the AI Search Search Profiles list with **State** set to **New**. An informational message and an alert triangle icon (⚠️) indicate that the new search profile has never been published.

To make content searchable using your new search profile, link one or more search sources to it. For instructions on linking search sources, see **Link a search source to a search profile**.

Your new search profile includes sample synonym and stop word dictionaries and a default typo handling dictionary. For more details on configuring and populating these dictionaries, see **Synonyms**, **Stop words**, and **Typo handling**.

**Link a search source to a search profile**

Link search sources to a search profile to specify the content users can search through that profile.

You must have already created at least one search source. For instructions on creating search sources, see **Create a search source**.

Role required: ais_admin

1. Navigate to **AI Search > Search Experience > Search Profiles**.
2. Edit the search profile that you want to link the search source to.
3. In the Search Sources related list, click **Link Existing**.
4. On the Search Profile - Search Source Mapping form, fill in the **Search source** field. Enter or look up the name for the search source you want to link to the search profile.
5. Click **Submit**.

The new search source appears in the Search Sources related list. Search query results immediately reflect changes to the set of records searchable through the search profile.
Derived auto-correction term lists for the search profile's typo handling dictionary do not automatically update to reflect changes to the set of searchable records. To update these auto-correction term lists, publish the search profile you edited. For details on publishing a search profile, see Publish a search profile.

**Publish a search profile**

Publish a search profile to make pending changes to its settings take effect in linked search applications.

Role required: ais_admin

To make a search profile's settings active in search queries, you must publish it. Publishing propagates the following settings to search application configurations that reference the search profile.

- The set of synonym and stop word dictionaries linked to the search profile
- Settings, blocked terms, and derived auto-correction terms for typo handling dictionaries linked to the search profile
- Result improvement rules and actions defined in the search profile

1. Navigate to **AI Search > Search Experience > Search Profiles**.

   **Note:** Search profiles with the **New** state display an alert triangle icon (⚠️). An informational message notifies you to publish these search profiles.

2. Edit the search profile that you want to publish.

3. Click **Publish**.

The search profile appears in the AI Search Search Profiles list with **State** set to **Published**.

**Synonyms**

Synonyms expand search queries to include additional terms with equivalent meaning or usage. Improve search recall by configuring synonym dictionaries and defining synonyms.

To define synonyms, modify the default synonym dictionary for a search profile or create a new synonym dictionary linked to one or more search profiles. Create and publish synonyms for each dictionary. Publish the dictionary to make your synonyms take effect for searches that use linked search profiles.

You can delete synonym dictionaries that are not linked to any search profiles.

**Synonym usage in search**

When a search query includes a term defined in a synonym, AI Search expands the search to include all equivalent terms defined in the synonym.

For example, a synonym might expand the search query term **vacation** to **vacation OR holiday OR pto**. The expanded query returns records that contain any of the three equivalent terms.

**Conditions for synonym eligibility**

To operate on a search query, a synonym must satisfy the following conditions:

- It must be active.
- It must be included in a published synonym dictionary.
- The parent synonym dictionary must be linked to the search profile specified for the search query.
- The language of the parent synonym dictionary must match the language of the search query.
Synonym terms and payloads

Each synonym includes two or more equivalent terms, defined in two fields. The Term field contains one term designated as the synonym's label. The Payload field contains the remaining equivalent terms, formatted as a JSON array.

Synonym term expansion is bidirectional. AI Search treats all terms defined in the Term and Payload fields as equivalent, as illustrated in the following table.

<table>
<thead>
<tr>
<th>Use case</th>
<th>Synonym expansion behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search query term matches the term from a synonym's Term field</td>
<td>AI Search expands the search query term to match all equivalent terms from the Payload field.</td>
</tr>
<tr>
<td>Search query term matches a term from the Payload field</td>
<td>AI Search expands the search query term to match the term from the Term field and all remaining equivalent terms from the Payload field.</td>
</tr>
</tbody>
</table>

Multi-word phrases

A synonym term can include either a single word or a multi-word phrase. AI Search expands multi-word phrases when the search query terms exactly match the order and proximity of the words in the synonym definition. If a user searches with these words in a different arrangement, no expansion occurs.

For example, the following table describes AI Search search expansion behavior for a synonym that includes the single word 401k and the multi-word phrase retirement account.

<table>
<thead>
<tr>
<th>Search query terms</th>
<th>Synonym expansion behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>401k</td>
<td>AI Search expands the search query to match either 401k or retirement account.</td>
</tr>
<tr>
<td>retirement account</td>
<td>AI Search expands the search query to match either 401k or retirement account.</td>
</tr>
<tr>
<td>retirement account bank</td>
<td>AI Search expands the search query to match either 401k or retirement account in addition to bank.</td>
</tr>
<tr>
<td>account retirement</td>
<td>AI Search does not expand the search query terms.</td>
</tr>
<tr>
<td>retirement bank account</td>
<td>AI Search does not expand the search query terms.</td>
</tr>
</tbody>
</table>

Case sensitivity

By default, synonym expansion ignores letter case when comparing synonyms with search query terms. You can enable case sensitivity for a synonym dictionary. This option affects all synonyms defined in the dictionary.

When case sensitivity is enabled, synonyms in the dictionary only match search query terms or phrases that include the same combination of uppercase and lowercase letters.

For example, if you define a synonym including the word CASE and the phrase Computer-Aided Software Engineering, AI Search expands searches for CASE but not searches for case.
**Punctuation sensitivity**

By default, synonym expansion ignores punctuation when comparing synonyms with search query terms. You can enable punctuation sensitivity for a synonym dictionary. This option affects all synonyms defined in the dictionary.

When punctuation sensitivity is enabled, synonyms in the dictionary only match search query terms or phrases that include the same punctuation.

For example, suppose you define a synonym equating U-S-A with University of South Australia and another synonym equating U.S.A. with United States of America. Without punctuation sensitivity enabled, a search for U.S.A. expands to match both University of South Australia and United States of America. When punctuation sensitivity is enabled, the same search only expands to match United States of America.

**Language dependence**

Synonym expansion is language-dependent. You specify a language for each synonym dictionary, and this language applies to all synonyms defined in the dictionary. Only synonyms from dictionaries with the same language as the search query are eligible for expansion.

AI Search supports synonym dictionaries for English, French Canada, French, German, Japanese, and Spanish.

**Interaction with other features**

The following table describes interactions between synonyms and other features that modify search queries or results.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Interaction with synonyms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Genius Results</td>
<td>Synonym expansion terms cannot trigger Genius Result configurations with Term trigger conditions.</td>
</tr>
<tr>
<td>Lemma and Unicode normalization</td>
<td>If a search query term is defined as a synonym, does not normalize it.</td>
</tr>
<tr>
<td>Result improvement rules</td>
<td>By default, a synonym expansion term can activate a result improvement rule if it matches the rule's Query trigger. You can prevent synonym expansion terms from activating a rule with a Query trigger by clearing the <strong>Expand Synonyms For Query Conditions</strong> option that appears when you define the Query trigger.</td>
</tr>
<tr>
<td>Stop words</td>
<td>If a synonym expands a search query's terms to include a term defined as a stop word, removes the stop word before computing results for the expanded search query. For example, suppose you define paas as a stop word and saas##paas as a synonym. If a user searches for saas, the synonym expands the search query term to saas OR paas, but removes the paas stop word before computing the search's results.</td>
</tr>
<tr>
<td>Typo handling</td>
<td>If a misspelled search query term is defined as a synonym, expands the synonym without auto-correcting it.</td>
</tr>
</tbody>
</table>
Publishing synonym dictionaries

Publishing a synonym dictionary makes its settings and active synonyms take effect in all linked search profiles.

Publishing a search profile updates the profile’s synonym dictionary links but does not update the dictionary’s settings or active synonyms in AI Search.

Create a synonym dictionary linked to a search profile

Define a new synonym dictionary and link it to a search profile.

Role required: ais_admin

To make a synonym dictionary affect search behavior, you must link it to a search profile, either at creation time or afterward. To learn about linking a saved dictionary to a search profile, see Link a synonym dictionary to a search profile.

1. Navigate to **AI Search > Search Experience > Search Profiles**.
2. Edit the search profile that you want to link the new synonym dictionary to.
3. In the Synonyms related list, click **Create and Link**.
4. On the form, fill in the fields.

### AI Search Dictionary form fields for synonym dictionary

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>Unique label for the synonym dictionary.</td>
</tr>
<tr>
<td>Dictionary name</td>
<td>Name for the synonym dictionary. This field is automatically set based on the <strong>Label</strong> field value.</td>
</tr>
<tr>
<td>Language</td>
<td>Language for all terms defined in the synonym dictionary.</td>
</tr>
<tr>
<td>Type</td>
<td>Dictionary type. This field is automatically set to <strong>Synonym</strong>.</td>
</tr>
<tr>
<td>State</td>
<td>Current state of the dictionary.</td>
</tr>
<tr>
<td></td>
<td>• <strong>New</strong>: The dictionary has never been published.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Draft</strong>: The dictionary is saved with unpublished changes.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Published</strong>: The dictionary is saved with all changes published.</td>
</tr>
<tr>
<td>Case sensitive</td>
<td>Option to enable case sensitivity for all synonyms in the dictionary.</td>
</tr>
<tr>
<td></td>
<td>For more details on case sensitivity, see <strong>Synonyms</strong>.</td>
</tr>
<tr>
<td>Punctuation sensitive</td>
<td>Option to enable punctuation sensitivity for all synonyms in the dictionary.</td>
</tr>
<tr>
<td></td>
<td>For more details on punctuation sensitivity, see <strong>Synonyms</strong>.</td>
</tr>
</tbody>
</table>

5. Click **Submit**.

The new synonym dictionary appears in the Synonyms related list.

To make new or updated synonym dictionary settings take effect, publish the search profile that you edited. For details on publishing a search profile, see **Publish a search profile**.
Create synonyms

Define terms to treat as equivalent in search queries.

Role required: ais_admin

You must have already created a synonym dictionary. For information on creating synonym dictionaries, see Create a synonym dictionary linked to a search profile.

1. Navigate to **AI Search > AI Search Engine > Dictionaries**.
2. Edit the synonym dictionary that you want to add the new synonym to.
3. In the AI Search Dictionary Terms related list, click **New**.
4. On the form, fill in the fields.

**AI Search Dictionary Term [Synonym view] form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dictionary</td>
<td>Name of the dictionary containing the synonym. This field is automatically</td>
</tr>
<tr>
<td></td>
<td>set based on the synonym dictionary you selected.</td>
</tr>
<tr>
<td>Term</td>
<td>Term to define as a synonym.</td>
</tr>
<tr>
<td>Payload</td>
<td>List of equivalent terms for the synonym, formatted as a JSON array of strings.</td>
</tr>
</tbody>
</table>

**Note:** If you enter an invalid JSON sequence in this field, an error message appears when you click **Submit**.

<table>
<thead>
<tr>
<th>State</th>
<th>Current state of the synonym record.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <strong>New:</strong> The synonym has never been published.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Draft:</strong> The synonym is saved with unpublished changes.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Published:</strong> The synonym is saved with all changes published.</td>
</tr>
</tbody>
</table>

| Active         | Option to activate the synonym for use in the synonym dictionary. To        |
|                | deactivate the synonym, clear the **Active** check box.                    |

5. Click **Submit**.

The new synonym appears in the AI Search Dictionary Terms related list.

6. Optional: Repeat the preceding steps for each additional synonym that you want to create.

7. Choose one of the following actions.

   • To save the modified dictionary and refresh its active synonyms in all linked search profiles, click **Publish**.
   • To save the modified dictionary without refreshing its active synonyms in all linked search profiles, click **Update**.

**Define a synonym with equivalent words and phrases**

This example shows a synonym defining *vacation*, *holiday*, *PTO*, and the phrase *time off* as equivalent.
Clone a synonym dictionary

Create a copy of an existing synonym dictionary.

Role required: ais_admin

Cloning a synonym dictionary copies the source dictionary's settings and all of its all defined synonym terms. This process can save you time when you need multiple synonym dictionaries that have many synonym terms in common.

1. Navigate to **AI Search > Search Query Settings > Dictionaries**.
2. Expand the Synonym record group if necessary and edit the synonym dictionary that you want to clone.
3. Click **Clone**.
4. In the Set Dictionary Label dialog box, enter a label for the new synonym dictionary in the **Cloned dictionary label** field and click **OK**.

The new synonym dictionary form opens. All synonym terms defined in the source dictionary appear in the AI Search Dictionary Terms related list.

Link a synonym dictionary to a search profile

Link an existing synonym dictionary to one or more search profiles.

Role required: ais_admin

You can link a single synonym dictionary to multiple search profiles.

1. Navigate to **AI Search > Search Experience > Search Profiles**.
2. Edit the search profile that you want to link the synonym dictionary to.
3. In the Synonyms related list, click **Link Existing**.
4. On the AI Search Profile Dictionary M2M form, follow these steps.
   a) Click the reference lookup icon (🔍) for the Dictionary field.
   b) Select the synonym dictionary that you want to link to the search profile.
   c) Click Submit.

The selected synonym dictionary appears in the search profile’s Synonyms related list.

To make the new synonym dictionary linking take effect, publish the search profile. For more information on publishing a search profile, see Publish a search profile.

Unlink a synonym dictionary from a search profile

Remove a synonym dictionary from a search profile.

Role required: ais_admin

Unlinking a synonym dictionary from a search profile does not delete the dictionary. To delete a synonym dictionary, you must first unlink it from all search profiles. For steps to delete a synonym dictionary, see Delete a synonym dictionary.

1. Navigate to AI Search > Search Experience > Search Profiles.
2. Edit the search profile that you want to unlink the synonym dictionary from.
3. In the Synonyms related list, select the option for the synonym dictionary that you want to unlink from the search profile.
4. Click Unlink Selected.

The selected synonym dictionary disappears from the search profile’s Synonyms related list.

To make the change in synonym dictionary linking take effect, publish the search profile. For more information on publishing a search profile, see Publish a search profile.

Delete a synonym dictionary

Remove a synonym dictionary that is not linked from any search profile.

Role required: ais_admin

1. Navigate to AI Search > Search Query Settings > Dictionaries.
   The AI Search Dictionaries list appears with a [Type] [!=] [Spell Check] filter condition applied and records grouped by dictionary type.
2. Expand the Synonym record group if necessary and edit the synonym dictionary that you want to delete.
3. Click Delete.

   **Note:** If the synonym dictionary is still linked to any search profiles, deletion fails and an error message lists the linked profiles. Unlink the dictionary from these search profiles, then repeat the preceding steps. For details on unlinking a synonym dictionary from a search profile, see Unlink a synonym dictionary from a search profile.

The selected synonym dictionary disappears from the AI Search Dictionaries list.

Stop words

Stop words remove search query terms that do not produce meaningful results. Improve search precision and relevancy by configuring stop word dictionaries and defining stop words.

Stop words are common terms that appear on a large proportion of indexed records. Examples of such terms can include articles, conjunctions, personal pronouns, and prepositions. By defining these terms as stop words, you can improve search precision and result relevancy for users.
You can define stop words in the default stop word dictionary for a search profile, or create your own stop word dictionaries linked to search profiles. Create and publish stop words for each dictionary. Publish the dictionary to make your stop words take effect for searches that use linked search profiles.

You can delete stop word dictionaries that are not linked to any search profiles.

**Stop word usage in search**

When a search query includes a term defined as a stop word, AI Search removes the term from the search query.

For example, a stop word might remove the term *my* from a search query for *upgrade my laptop*. This modified search query only matches records containing the more relevant terms *upgrade* and *laptop*.

**Conditions for stop word eligibility**

To operate on a search query, a stop word must meet these conditions:

- It must be active.
- It must be included in a published stop word dictionary.
- The parent stop word dictionary must be linked to the search profile specified for the search query.
- The language of the parent stop word dictionary must match the language of the search query.

**Multi-word phrases**

A stop word term can include either a single word or a multi-word phrase. AI Search removes multi-term phrases when the words in the search query exactly match the order and proximity of the words in the stop word definition. If a user searches with these words in a different arrangement, no term removal occurs.

For example, if you define a *retirement account* stop word, AI Search removes these terms from a search for *401k retirement account* but does not remove them from a search for *retirement 401k account*.

**Case sensitivity**

By default, AI Search ignores letter case when comparing stop words with search query terms. You can enable case sensitivity for a stop word dictionary. This option affects all stop words defined in the dictionary.

When case sensitivity is enabled, stop words in the dictionary only match search query terms or phrases that include the same combination of uppercase and lowercase letters.

For example, if you define a *RAID* stop word in a dictionary with case sensitivity enabled, AI Search ignores the search query term *RAID* but treats the search query term *raid* normally.

**Punctuation sensitivity**

By default, AI Search ignores punctuation when comparing stop words with search query terms. You can enable punctuation sensitivity for a stop word dictionary. This option affects all stop words defined in the dictionary.

When punctuation sensitivity is enabled, stop words in the dictionary only match search query terms or phrases that include the same punctuation.

For example, if you define a *one-half* stop word in a dictionary with punctuation sensitivity enabled, AI Search removes the search query term *one-half* but does not remove the search query term *one half*. 
Language dependence

Stop word removal is language-dependent. You specify a language for each stop word dictionary, and this language applies to all stop words defined in the dictionary. Only stop words from dictionaries with the same language as the search query are eligible for removal.

AI Search supports stop word dictionaries for English, French Canada, French, German, Japanese, and Spanish. You can only link one stop word dictionary per language to a given search profile.

Interaction with other features

The following table describes interactions between stop words and other features that modify search queries or results.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Interaction with stop words</th>
</tr>
</thead>
<tbody>
<tr>
<td>Genius Results</td>
<td>If a search query term that matches a Genius Result configuration's Term trigger is defined as a stop word, evaluates the trigger before removing the stop word from the search query.</td>
</tr>
<tr>
<td>Lemma and Unicode normalization</td>
<td>If a search query term is defined as a stop word, removes the term without normalizing it.</td>
</tr>
<tr>
<td>Result improvement rules</td>
<td>If a search query term that matches a result improvement rule's Query trigger is defined as a stop word, evaluates the rule trigger before removing the stop word from the search query.</td>
</tr>
</tbody>
</table>
| Synonyms                       | If a synonym expands a search query's terms to include a term defined as a stop word, removes the stop word before computing results for the expanded search query.  
                                    For example, suppose you define paas as a stop word and saas##paas as a synonym. If a user searches for saas, the synonym expands the search query term to saas OR paas, but removes the paas stop word before computing the search's results. |
| Typo handling                  | If a misspelled search query term is defined as a stop word, auto-corrects the term normally instead of removing it. Ignores terms defined as stop words when determining an auto-correction for a misspelled search query term. For example, if you define email as a stop word, does not offer email as an auto-correction when you search for emial. |

Publishing stop word dictionaries

Publishing a stop word dictionary makes its settings and active stop words take effect in all linked search profiles.

Publishing a search profile updates the profile's stop word dictionary links but does not update the dictionary's settings or active stop words in AI Search.

Create a stop word dictionary linked to a search profile
Define a new stop word dictionary and link it to a search profile.

Role required: ais_admin

To make a stop word dictionary affect search behavior, you must link it to a search profile, either at creation time or afterward. You can only link one stop word dictionary per language to a given search profile. To learn about linking a saved stop word dictionary to a search profile, see Link a stop word dictionary to a search profile.

1. Navigate to **AI Search > Search Experience > Search Profiles**.
2. Edit the search profile that you want to link the new stop word dictionary to.
3. In the Stop Words related list, click **Create and Link**.
4. On the form, fill in the fields.

### Dictionary form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>Unique label for the dictionary.</td>
</tr>
<tr>
<td>Dictionary name</td>
<td>Name for the dictionary. This field is automatically set based on the <strong>Label</strong> field value.</td>
</tr>
<tr>
<td>Language</td>
<td>Language for all stop words defined in the dictionary. AI Search only considers stop words with the same language as the search query. You can only link one stop word dictionary with a given language to a search profile.</td>
</tr>
<tr>
<td>Type</td>
<td>Dictionary type. This field is automatically set to <strong>Stop Word</strong>.</td>
</tr>
<tr>
<td>State</td>
<td>Current state of the dictionary.</td>
</tr>
<tr>
<td></td>
<td>• <strong>New</strong>: The dictionary has never been published.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Draft</strong>: The dictionary is saved with unpublished changes.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Published</strong>: The dictionary is saved with all changes published.</td>
</tr>
<tr>
<td>Case sensitive</td>
<td>Option to enable case sensitivity for all stop words in the dictionary. For more details on case sensitivity, see <strong>Stop words</strong>.</td>
</tr>
<tr>
<td>Punctuation sensitive</td>
<td>Option to enable punctuation sensitivity for all stop words in the dictionary. For more details on punctuation sensitivity, see <strong>Stop words</strong>.</td>
</tr>
</tbody>
</table>

5. To save the new stop word dictionary and link it to the specified search profile, click **Submit**.

The new stop word dictionary appears in the Stop Words related list.

To make new or updated stop word dictionary settings take effect, publish the search profile that you edited. For details on publishing a search profile, see Publish a search profile.

Create stop words

Define terms to remove from search queries.

Role required: ais_admin
You must have already created a stop word dictionary. For information on creating stop word dictionaries, see Create a stop word dictionary linked to a search profile.

1. Navigate to **AI Search > AI Search Engine > Dictionaries**.
2. Edit the stop word dictionary that you want to add the new stop word to.
3. In the AI Search Dictionary Terms related list, click **New**.
4. On the form, fill in the fields.

### Dictionary Term form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dictionary</td>
<td>Name of the dictionary containing the stop word. This field is automatically set based on the stop word dictionary that you selected.</td>
</tr>
<tr>
<td>Term</td>
<td>Term to define as a stop word.</td>
</tr>
<tr>
<td>Active</td>
<td>Option to activate the stop word for use in the stop word dictionary. To deactivate the stop word, clear the <strong>Active</strong> check box.</td>
</tr>
</tbody>
</table>

5. Click **Submit**.
   The new stop word appears in the AI Search Dictionary Terms related list.

6. Optional: Repeat the preceding steps for each additional stop word that you want to create.

7. Choose one of the following actions.
   - To save the modified dictionary and refresh its active stop words in all linked search profiles, click **Publish**.
   - To save the modified dictionary without refreshing its active stop words in all linked search profiles, click **Update**.

### Clone a stop word dictionary

Create a copy of an existing stop word dictionary.

Role required: ais_admin

Cloning a stop word dictionary copies the source dictionary's settings and all of its all defined stop word terms. This process can save you time when you need multiple stop word dictionaries that have many stop word terms in common.

1. Navigate to **AI Search > Search Query Settings > Dictionaries**.
2. Expand the Stop Word record group if necessary and edit the stop word dictionary that you want to clone.
3. Click **Clone**.
4. In the Set Dictionary Label dialog box, enter a label for the new stop word dictionary in the **Cloned dictionary label** field and click **OK**.

The new stop word dictionary form opens. All stop word terms defined in the source dictionary appear in the AI Search Dictionary Terms related list.

### Link a stop word dictionary to a search profile

Link an existing stop word dictionary to one or more search profiles.

Role required: ais_admin

You can link a single stop word dictionary to multiple search profiles. You can only link one stop word dictionary per language to a given search profile.

1. Navigate to **AI Search > Search Experience > Search Profiles**.
2. Edit the search profile that you want to link the stop word dictionary to.
3. In the Stop Words related list, click **Link Existing**.
4. On the AI Search Profile Dictionary M2M form, follow these steps.
   a) Click the reference lookup icon (🔍) for the Dictionary field.
   b) Select the stop word dictionary that you want to link to the search profile.
   c) Click Submit.

The selected stop word dictionary appears in the search profile's Stop Words related list.

To make the new stop word dictionary linking take effect, publish the search profile. For more information on publishing a search profile, see Publish a search profile.

Unlink a stop word dictionary from a search profile

Remove a stop word dictionary that is not linked from any search profile.

Role required: ais_admin

Unlinking a stop word dictionary from a search profile does not delete the dictionary. To delete a stop word dictionary, you must first unlink it from all search profiles. For steps to delete a stop word dictionary, see Delete a stop word dictionary.

1. Navigate to AI Search > Search Experience > Search Profiles.
2. Edit the search profile that you want to unlink the stop word dictionary from.
3. In the Stop Words related list, select the option for the stop word dictionary that you want to unlink from the search profile.
4. Click Unlink Selected.

The selected stop word dictionary disappears from the search profile's Stop Words related list.

To make the change in stop word dictionary linking take effect, publish the search profile. For more information on publishing a search profile, see Publish a search profile.

Delete a stop word dictionary

Remove a stop word dictionary that is not linked from any search profile.

Role required: ais_admin

1. Navigate to AI Search > Search Query Settings > Dictionaries.
   The AI Search Dictionaries list appears with a [Type] [!=] [Spell Check] filter condition applied and records grouped by dictionary type.
2. Expand the Stop Word record group if necessary and edit the stop word dictionary that you want to delete.
3. Click Delete.

   Note: If the stop word dictionary is still linked to any search profiles, deletion fails and an error message lists the linked profiles. Unlink the dictionary from these search profiles, then repeat the preceding steps. For details on unlinking a stop word dictionary from a search profile, see Unlink a synonym dictionary from a search profile.

The selected stop word dictionary disappears from the AI Search Dictionaries list.

Typo handling

AI Search replaces misspelled search query terms with auto-correction terms derived from indexed content. Configure typo handling dictionary settings to control derivation of auto-correction terms.

To define auto-correction terms for a search profile, modify settings in the profile's linked typo handling dictionary. The typo handling dictionary derives a list of auto-correction terms from indexed content found in search sources linked to its search profile. Update the typo handling dictionary to save its settings. Publish the linked search profile to make auto-correction terms available for searches that use the profile.
AI Search automatically creates a typo handling dictionary for a search profile when you link search sources to that profile. You cannot delete a typo handling dictionary, unlink it from its search profile, or link it to any other search profile.

To disable typo handling auto-correction for a search application, deselect the **Enable Typo Handling** option in the search application configuration. For more details on search application configuration settings, see [Create a search application configuration for AI Search](#).

**Conditions for auto-correction term eligibility**

When deriving its list of auto-correction terms, the typo handling dictionary only considers indexed terms that satisfy the following conditions:

- The term includes at least 3 characters and no more than 255 characters.
- The term appears at least once in indexed records from the search profile's linked search sources.

**Auto-correction of search query terms**

When a search query includes a term not present in the typo handling dictionary, AI Search looks for terms in the dictionary with similar spelling. If it finds a good match, it automatically replaces the original search query term with the dictionary term.

For example, a search for `emial`, which is not present on any indexed record, might auto-correct to the similarly spelled term `email` which exists on multiple indexed records and thus appears in the typo handling dictionary.

A notification message displays the auto-corrected term. Users can click the link in this message to repeat their search with the original query term.

**Showing results for email**

*Search instead for emial*

**Terms excluded from auto-correction**

Auto-correction ignores search query terms that satisfy any of the following conditions:

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search query term less than 3 characters in length</td>
<td>Auto-correction ignores search query terms below 3 characters in length.</td>
</tr>
<tr>
<td></td>
<td>For example, AI Search does not auto-correct the search query term <code>gi</code>.</td>
</tr>
<tr>
<td>Search query term includes only uppercase letters</td>
<td>To enable search for abbreviations, auto-correction ignores search query</td>
</tr>
<tr>
<td></td>
<td>terms that contain only uppercase letters.</td>
</tr>
<tr>
<td></td>
<td>For example, AI Search does not auto-correct the search query term <code>PINN</code>,</td>
</tr>
<tr>
<td></td>
<td>even if it auto-corrects the lowercase form <code>pinn</code> to <code>pin</code>.</td>
</tr>
<tr>
<td>Condition</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Search query term includes one or more numeric digits</td>
<td>To enable search for numbers and alphanumeric identifiers, auto-correction ignores search query terms that include numeric digits. For example, AI Search does not auto-correct the search query term 4 0 2 K.</td>
</tr>
<tr>
<td>Search query term excluded from typo handling dictionary</td>
<td>Auto-correction ignores search query terms excluded from the typo handling dictionary. For instructions on excluding terms from a typo handling dictionary, see Exclude a term from a typo handling dictionary.</td>
</tr>
</tbody>
</table>

**Automatic refresh of auto-correction term lists**

Each typo handling dictionary automatically refreshes its list of auto-correction terms after a set interval. The refresh operation has the same effect as republishing the dictionary's linked search profile.

By default, typo handling dictionaries refresh every 24 hours. If you want the term list refreshed less frequently, you can increase this interval in the dictionary settings.

**Language dependence**

Typo handling is language-dependent. AI Search derives a separate list of auto-correction terms for each supported language found in the search sources' indexed content.

AI Search supports derivation of auto-correction terms for English, French Canada, French, German, and Spanish. Typo handling auto-correction term derivation is not supported for Japanese.

**Interaction with other features**

The following table describes interactions between typo handling and other features that modify search queries or results.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Interaction with typo handling</th>
</tr>
</thead>
<tbody>
<tr>
<td>Genius Results</td>
<td>Auto-corrected search query terms cannot trigger Genius Result configurations with Term trigger conditions.</td>
</tr>
<tr>
<td>Lemma and Unicode normalization</td>
<td>performs lemma and Unicode normalization on auto-corrected search query terms.</td>
</tr>
<tr>
<td>Result improvement rules</td>
<td>An auto-corrected search query term can trigger a result improvement rule if it matches the rule's Query trigger.</td>
</tr>
</tbody>
</table>
Feature | Interaction with typo handling
--- | ---
Stop words | If a misspelled search query term is defined as a stop word, auto-corrects the term normally instead of removing it. Ignores terms defined as stop words when determining an auto-correction for a misspelled search query term. For example, if you define `email` as a stop word, does not offer `email` as an auto-correction when you search for `email`.

Synonyms | If a misspelled search query term is defined as a synonym, expands the synonym without auto-correcting it.

Modify settings for a typo handling dictionary
Modify typo handling dictionary settings for a search profile.

Role required: ais_admin

Each typo handling dictionary is linked to a search profile. For more information about search profiles, see Search profiles.

1. Navigate to **AI Search > Search Experience > Search Profiles**.
2. Edit the search profile that contains the typo handling dictionary that you want to modify.
3. In the Typo Handling related list, edit the record for the typo handling dictionary.
4. On the form, update the fields.

### AI Search Dictionary form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>Unique label for the typo handling dictionary.</td>
</tr>
<tr>
<td>Dictionary name</td>
<td>Name for the typo handling dictionary. This field is automatically set based on the initial <code>Label</code> field value.</td>
</tr>
<tr>
<td>Type</td>
<td>Dictionary type. This field is automatically set to Spell Check.</td>
</tr>
<tr>
<td>State</td>
<td>Current state of the dictionary.</td>
</tr>
<tr>
<td></td>
<td>• <strong>New</strong>: The dictionary has never been published.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Draft</strong>: The dictionary is saved with unpublished changes.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Published</strong>: The dictionary is saved with all changes published.</td>
</tr>
<tr>
<td></td>
<td>This field is automatically set.</td>
</tr>
<tr>
<td>Case sensitive</td>
<td>Option to enable case sensitivity for all auto-correction terms in the dictionary. For more details on case sensitivity, see Typo handling.</td>
</tr>
<tr>
<td>Punctuation sensitive</td>
<td>Option to enable punctuation sensitivity for all auto-correction terms in the dictionary. For more details on punctuation sensitivity, see Typo handling.</td>
</tr>
</tbody>
</table>
## Field | Description
--- | ---
**Derived** | Option to derive dictionary entries from indexed content. This field is automatically set.

**Derive Settings**

| **Indexed sources** | List of indexed sources. The dictionary derives auto-correction terms from content indexed for these sources. For more information on indexed sources, see Indexed sources. |

| **Auto refresh** | Interval, in hours, after which derived typo handling entries automatically refresh. The minimum value is 24 hours. |

**Blocked Fields**

| | Comma-separated list of fields. The dictionary excludes terms found in these fields when deriving typo handling auto-correction terms from indexed source records. You can specify fields using the following formats: |
| | • * (asterisk): Exclude terms found in all fields. This value disables derivation of typo-handling auto-corrections for the dictionary. |
| | • `fieldname`: Exclude terms found in the specified AI Search index field, such as `title` or `text`. For details on AI Search index fields, see AI Search index fields. |
| | • `tablename.fieldname`: Exclude terms found in the specified field on the specified Now Platform table. |
| | • `tablename.*`: Exclude terms found in all fields in the specified Now Platform table. |

---

5. **Click Update.**

To make updated settings for a typo handling dictionary take effect, publish the search profile linked to the dictionary. For details on publishing a search profile, see Publish a search profile.

**Exclude a term from a typo handling dictionary**

Prevent AI Search from auto-correcting a term in user search queries by excluding the term from a typo handling dictionary.

You must have already defined a search profile with one or more linked search sources.

Role required: ais_admin

1. Navigate to **AI Search > Search Experience > Search Profiles.**
2. Edit the search profile that you want to exclude a typo handling term for.
3. In the Typo Handling related list, edit the typo handling dictionary.
4. In the AI Search Dictionary Terms related list, click **New.**
5. On the form, fill in the fields.

### Dictionary Term form

<table>
<thead>
<tr>
<th><strong>Field</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dictionary</strong></td>
<td>Typo handling dictionary that the term exclusion applies to. This field is automatically set.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Term</td>
<td>Term that you want auto-correction to ignore in user search queries.</td>
</tr>
<tr>
<td>Application</td>
<td>Application scope for the term exclusion. This field is automatically set.</td>
</tr>
<tr>
<td>Active</td>
<td>Option to activate the term exclusion for the typo handling dictionary.</td>
</tr>
<tr>
<td>Marked for Deletion</td>
<td>Option indicating that AI Search will delete the term exclusion the next time you publish the search profile linked to the typo handling dictionary. This field is automatically set.</td>
</tr>
</tbody>
</table>

6. Click **Submit**.

The new term appears in the AI Search Dictionary Terms related list with the **State** set to **New**.

7. Optional: Repeat the preceding steps for each additional term that you want to exclude.

8. Click **Publish**.

The typo handling dictionary appears in the Typo Handling related list with the **State** set to **Published**.

To make updated typo handling settings take effect, publish the search profile that you edited. For details on publishing a search profile, see **Publish a search profile**.

**Genius Results**

Optionally display the best answers for a search query as actionable Genius Result cards included with search results.

**Note:** Genius Results are not enabled in the base system. To use Genius Results, you must manually enable them. For instructions on enabling Genius Results in your instance, see **Train and publish the NLU model for default Genius Result configurations** and **Enable Genius Results**.

A Genius Result configuration includes a trigger condition and logic for creating answers. The trigger condition determines whether the Genius Result configuration activates for a search query. When a configuration activates, its answer logic populates one or more Genius Result cards with information and actions. These Genius Result cards are displayed with the list of results for the search query, giving the user immediate access to answers and actions.

**Genius Result trigger conditions**

You can select any one of the following trigger conditions for a Genius Result configuration:

- **Always**: The Genius Result configuration activates for all search queries.
- **NLU**: The Genius Result configuration activates when the search query’s detected intent matches a specified NLU model intent. For more information on NLU models and intents, see **Natural Language Understanding**.
- **Term**: The Genius Result configuration activates when the search query consists of a single specified term or phrase.

**Genius Result answer types**

A Genius Result configuration can include either of the following answer types:

- **Search**: When triggered, displays Genius Result cards for up to three results from a search query defined by a server-side script in the Genius Result configuration. Each search result displays as a separate Genius Result card. If the search query returns no results, no Genius Result card is displayed.
• **Script**: When triggered, displays a Genius Result card containing key-value pairs from an object defined by a server-side script in the Genius Result configuration. The script can use methods from any Now Platform public API to construct this object.

### Language support

In the Quebec release, Genius Results only support English search queries.

### NLU model row limit for Genius Results

By default, Genius Result configurations with NLU trigger conditions only consider a maximum of 100,000 randomly selected records from their target table. As a result, they may not display all matches from large target tables.

You can override this default limit by modifying the value of the **Maximum number of records in a Table vocabulary source** NLU Workbench system property (glide.platform_ml.api.max_nlu_lookupsource_records).

**Warning**: Be careful when increasing this limit beyond the default value, as higher values may affect performance of search queries and other functions that rely on NLU matching.

For more information on NLU Workbench system properties, see NLU Workbench properties.

### Interaction with other features

The following table describes interactions between Genius Results and other features that modify search queries or results.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Interaction with Genius Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lemma and Unicode normalization</td>
<td>Search query terms added by lemma or Unicode normalization cannot trigger Genius Result configurations with Term trigger conditions.</td>
</tr>
<tr>
<td>Stop words</td>
<td>If a search query term that matches a Genius Result configuration’s Term trigger is defined as a stop word, evaluates the trigger before removing the stop word from the search query.</td>
</tr>
<tr>
<td>Synonyms</td>
<td>Synonym expansion terms cannot trigger Genius Result configurations with Term trigger conditions.</td>
</tr>
<tr>
<td>Typo handling</td>
<td>Auto-corrected search query terms cannot trigger Genius Result configurations with Term trigger conditions.</td>
</tr>
</tbody>
</table>

Train and publish the NLU model for default Genius Result configurations

Train and publish the NLU model used by default Genius Result configurations with NLU triggers.

Role required: admin or nlu_admin

Some of the default Genius Result configurations have NLU triggers. These configurations rely on intents defined in an AI Search NLU model. To make this model available for use in Genius Result configurations, sync its vocabulary sources, then train and publish it.

1. Navigate to NLU Workbench > Vocabulary Sources.
2. In the **ServiceNow Tables** tab, for each vocabulary source used in the Default AI Search Genius Results Model, point to the empty last column and click **Sync**.

**Vocabulary sources**

<table>
<thead>
<tr>
<th>Vocabulary handle</th>
<th>Source table</th>
<th>Source field</th>
<th>Used in</th>
<th>Last refresh</th>
<th>Current status</th>
<th>Refresh</th>
</tr>
</thead>
<tbody>
<tr>
<td>#CatalogItem</td>
<td>Catalog Item</td>
<td>Name</td>
<td>Default AI Search Genius Results Model</td>
<td>-</td>
<td>Never synced</td>
<td>Every 7 days</td>
</tr>
<tr>
<td>RightLocation</td>
<td>Location</td>
<td>City</td>
<td>Default AI Search Genius Results Model</td>
<td>-</td>
<td>Never synced</td>
<td>Every 7 days</td>
</tr>
</tbody>
</table>

The current status of each vocabulary source changes to **Syncing**. When sync is complete, it changes to **Synced**.

![Sync button](image)

**Note:** The system may take a few hours to complete initial sync for a vocabulary source. Later sync operations for the vocabulary source complete faster, in minutes or seconds.

3. Navigate to **NLU Workbench > Models**.
4. Edit the record for the Default AI Search Genius Results Model.
5. Click **Train**.
   The **Test model** and **Train and publish** tabs appear in a new pane.
6. In the **Train and publish** tab, click **Train**.

**Note:** Depending on the amount of data in your instance, the system may take some time to train the NLU model.

An informational message indicates that training completed successfully.

7. In the **Train and publish** tab, click **Publish**.
   The **Publish UI Model** dialog box appears.
8. In the **Publish UI Model** dialog box, click **Publish**.

**Note:** Depending on the amount of data in your instance, the system may take some time to publish the NLU model.

An informational message indicates that publishing completed successfully.

Genius Result configurations can use the Default AI Search Genius Results Model. The system retrains and republishes this NLU model every seven days.

Publish any search profiles that include Genius Results, then follow the steps in **Enable Genius Results** to activate Genius Results for your search queries.

Enable Genius Results
Genius Results are not enabled in the base system. To use Genius Results, you must manually enable them.

If you intend to use Genius Results configurations with NLU triggers, follow the steps from **Train and publish the NLU model for default Genius Result configurations** before performing this task.

Role required: admin
To enable Genius Results in your instance, set the value of the glide.ais.genius_result.enabled system property to true.

1. In the filter navigator, enter sys_properties.list and press Enter.
2. Edit the glide.ais.genius_result.enabled system property.
3. Change the system property’s value to true.
4. Click Update.

Train and publish the NLU model for default Genius Result configurations

Train and publish the NLU model used by default Genius Result configurations with NLU triggers.

Role required: admin or nlu_admin

Some of the default Genius Result configurations have NLU triggers. These configurations rely on intents defined in an AI Search NLU model. To make this model available for use in Genius Result configurations, sync its vocabulary sources, then train and publish it.

1. Navigate to NLU Workbench > Vocabulary Sources.
2. In the ServiceNow Tables tab, for each vocabulary source used in the Default AI Search Genius Results Model, point to the empty last column and click Sync.

Vocabulary sources

<table>
<thead>
<tr>
<th>Vocabulary handle</th>
<th>Source table</th>
<th>Source field</th>
<th>Used In</th>
<th>Last refresh</th>
<th>Current status</th>
<th>Refresh</th>
</tr>
</thead>
<tbody>
<tr>
<td>@ActionItem</td>
<td>Catalog Item</td>
<td>Name</td>
<td>Default AI Search Genius Results Model</td>
<td>Never synced</td>
<td>Every 7 days</td>
<td>Sync</td>
</tr>
<tr>
<td>@ActionLocation</td>
<td>Location</td>
<td>City</td>
<td>Default AI Search Genius Results Model</td>
<td>Never synced</td>
<td>Every 7 days</td>
<td></td>
</tr>
</tbody>
</table>

The current status of each vocabulary source changes to Syncing. When sync is complete, it changes to Synced.

Note: The system may take a few hours to complete initial sync for a vocabulary source. Later sync operations for the vocabulary source complete faster, in minutes or seconds.

4. Edit the record for the Default AI Search Genius Results Model.
5. Click Train.

The Test model and Train and publish tabs appear in a new pane.

6. In the Train and publish tab, click Train.

Note: Depending on the amount of data in your instance, the system may take some time to train the NLU model.

An informational message indicates that training completed successfully.

7. In the Train and publish tab, click Publish.

The Publish UI Model dialog box appears.
8. In the Publish UI Model dialog box, click Publish.

Note: Depending on the amount of data in your instance, the system may take some time to publish the NLU model.

An informational message indicates that publishing completed successfully.

Genius Result configurations can use the Default AI Search Genius Results Model. The system retrain and republishes this NLU model every seven days.

Publish any search profiles that include Genius Results, then follow the steps in Enable Genius Results to activate Genius Results for your search queries.

Default Genius Result configurations

Pre-configured AI Search Genius Result configurations display actionable top results for People, Catalog Item, and Q&A search queries.

You can link these default Genius Result configurations to your own search profiles. You cannot modify the default Genius Result configurations, but you can clone them and modify the cloned configurations.

Catalog Item - EN

The Catalog Item - EN Genius Result configuration displays top search results from the Catalog Item [sc_cat_item] table. Each answer card shows a single CI record.

Sample Catalog Item - EN answer card

Click the answer card's Request Item action link to create a new request for the specified CI.

People - EN

The People - EN Genius Result configuration displays top search results from the User [sys_user] table. Each answer card shows a single user record.
Sample People - EN answer card

Click the answer card’s View profile action link to see the user’s profile, or click the View org chart action link to view the user’s organization chart.

Q&A

The Q&A Genius Result configuration displays top search results extracted from HTML fields of records on the Knowledge [kb_knowledge] table and tables that extend it. Each answer card shows a topic and answer pair extracted from a single Knowledge article.

Sample Q&A answer card

Click the answer card’s View Article action link to view the full Knowledge article.

Topic and answer extraction for Q&A Genius Results

By default, AI Search automatically determines which elements of a Knowledge article’s HTML field values to extract as the Q&A topic and answer. You cannot configure the criteria for this extraction behavior.

Topic and answer extraction behavior varies depending on the table that contains the Knowledge article:
Knowledge article source | Q&A heuristic extraction
---|---
FAQ [kb_template_faq] table | AI Search heuristically extracts the Q&A topic from the Knowledge article record's Question HTML field. It extracts the Q&A answer from the record's Answer HTML field.

**Note:** This table is enabled when you activate the Knowledge Management Advanced plugin (com.snc.knowledge_advanced). For more information, see Activate the Knowledge Management Advanced plugin.

Knowledge [kb_knowledge] table and all other tables that extend it | AI Search heuristically extracts the Q&A topic and answer from the Knowledge article record's HTML fields.

You can override the extraction heuristics for a Knowledge article by manually designating a topic and an answer in that article's HTML fields. To do so, set the HTML classes described in the following table on elements in the article's HTML fields.

<table>
<thead>
<tr>
<th>HTML Class</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>class=&quot;sn_snippet_topic&quot;</td>
<td>Set this class on the HTML field element that contains text you want to designate as the Q&amp;A Genius Result topic for the Knowledge article.</td>
</tr>
<tr>
<td>class=&quot;sn_snippet_answer&quot;</td>
<td>Set this class on the HTML element that contains text that you want to designate as the Q&amp;A Genius Result answer for the Knowledge article.</td>
</tr>
</tbody>
</table>

**Note:** Answer text should be from 250 to 300 characters in length. Longer answers may be cut off when displayed on the Q&A Genius Results card.

Link a Genius Result configuration to a search profile

Link a Genius Result configuration to one or more search profiles.

Role required: ais_admin

You can link a single Genius Result configuration to multiple search profiles.

1. Navigate to **AI Search > Search Experience > Search Profiles**.
2. Edit the search profile that you want to link the Genius Result configuration to.
3. In the Genius Results related list, click **Link Existing**.
4. On the form, fill in the fields.

**Search Profile - Genius Result Mapping form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
<td>The search profile to link the Genius Result configuration to. This field is automatically set to the profile that you edited.</td>
</tr>
<tr>
<td>Genius Result Configuration</td>
<td>The Genius Result configuration to link to the specified search profile.</td>
</tr>
<tr>
<td>Order</td>
<td>Order of evaluation for the Genius Result configuration in the context of the search profile.</td>
</tr>
</tbody>
</table>
Create a Genius Result configuration

Role required: ais_admin

1. Navigate to **AI Search > Search Experience > Search Profiles**.
2. Edit the search profile that you want to link the new Genius Result configuration to.
3. In the Genius Results related list, click **Create and Link**.
4. On the form, fill in the fields.

**AI Search Genius Result Configuration form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name for the Genius Result configuration.</td>
</tr>
</tbody>
</table>

5. Click **Submit**.

The new Genius Result configuration appears in the Genius Results related list.

---

The new Genius Result configuration appears in the Genius Results related list.

Create a Genius Result configuration

Create a Genius Result configuration, set its trigger condition, and configure the results displayed on its answer card.

Role required: ais_admin

1. Navigate to **AI Search > Search Experience > Search Profiles**.
2. Edit the search profile that you want to link the new Genius Result configuration to.
3. In the Genius Results related list, click **Create and Link**.
4. On the form, fill in the fields.

**AI Search Genius Result Configuration form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name for the Genius Result configuration.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Trigger condition</td>
<td>Condition that triggers evaluation of the Genius Result configuration. Supported values:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Always</strong>: The Genius Result configuration triggers for every search query.</td>
</tr>
<tr>
<td></td>
<td>• <strong>NLU</strong>: The Genius Result configuration triggers when the search query’s detected intent matches an NLU model intent. To use this trigger condition, you must link the NLU model and one or more of its intents to your Genius Result configuration. For instructions, see Link an NLU model and intents to a Genius Result configuration.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For an NLU trigger condition to function, the NLU model must be published. You can verify NLU model status by navigating to <strong>AI Search &gt; Search Query Settings &gt; Search Intents</strong>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Term</strong>: The Genius Result configuration triggers when the search query exactly matches a specified set of query terms.  <strong>Note:</strong> Exact matching means that the search query must contain only the specified terms in the specified order. For example, if you define <code>conference room</code> as the trigger term, a search for <code>conference room</code> triggers the Genius Result condition but searches for <code>hotel conference room</code> or <code>room conference</code> do not trigger it.</td>
</tr>
<tr>
<td>Term</td>
<td>Term that triggers the Genius Result configuration when it exactly matches the search query. This field appears only when you select <strong>Term</strong> from the <strong>Trigger condition</strong> field.</td>
</tr>
<tr>
<td>Application</td>
<td>Application scope for the Genius Result configuration. This field is automatically set.</td>
</tr>
<tr>
<td>Active</td>
<td>Option to enable the Genius Result configuration. Inactive Genius Result configurations never trigger.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Genius result answer type</td>
<td>Type of answer the Genius Result configuration should return when triggered by a search query. Supported values:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Search</strong>: Displays Genius Result cards for up to three results from a search query. You define this search query in an answer object using server-side script logic in the Genius result logic field. Each search result is displayed as a separate Genius Result card. If the search query returns no results, no Genius Result card is displayed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Script</strong>: Displays a Genius Result card containing arbitrary field names and values (key-value pairs). You add these fields to an answer object using server-side script logic in the Genius result logic field. The script can use methods from any Now Platform public API to construct this object.</td>
</tr>
<tr>
<td>Genius result logic</td>
<td>Server-side script function that takes a query context object as its parameter. This script returns a GeniusResultAnswer object used to populate Genius Result answer cards. The required structure for the answer object varies by Genius Result answer type:</td>
</tr>
<tr>
<td></td>
<td>• For the <strong>Search</strong> answer type, the GeniusResultAnswer object must define a search query using the GeniusResultAnswer.setTable(), GeniusResultAnswer.addSearchPhrases(), and GeniusResultAnswer setSearchPhrase() API methods. Each result from the search query is displayed as a separate Genius Result answer card, to a maximum of three results.</td>
</tr>
<tr>
<td></td>
<td>• For the <strong>Script</strong> answer type, the GeniusResultAnswer object must define a map of key-value pairs using the GeniusResultAnswer.addDataMap() API method. Each key-value pair represents a field name and value that you want the Genius Result answer card to display.</td>
</tr>
<tr>
<td></td>
<td>For descriptions of API methods usable in this script function, see the GeniusResultAnswer and GeniusResultContext scoped JavaScript API descriptions.</td>
</tr>
</tbody>
</table>
Return fields

Comma-separated list of fields to display on the Genius Result answer card. Behavior varies by Genius Result answer type:

- For the **Search** answer type, the answer card automatically displays the common AI Search index fields:
  - ai_search_parent_title
  - ai_search_teaser_text
  - ai_search_teaser_title
  - record_class_name
  - sys_id
  - table

Use this field to specify any additional AI Search index fields that you want to display for search results on the Genius Result answer cards.

To view the list of AI Search index fields, see [AI Search index fields](#).

- For the **Script** answer type, use this field to specify the names of fields defined in the GeniusResultAnswer object that you want to display on the Genius Result answer card.

5. Click **Submit**.
   The new Genius Result configuration appears in the Genius Results related list.

6. Optional: Edit the **Order** for the new Genius Result configuration to control its display order for the search profile.

Changes to Genius Result configurations take effect in search as soon as you save them. You do not need to publish the linked search profile to make the new configuration take effect.

If you selected an **NLU** trigger condition, you must link an NLU model and its intents to your Genius Result configuration. For instructions, see [Link an NLU model and intents to a Genius Result configuration](#).

Link an NLU model and intents to a Genius Result configuration
Specify the NLU model and intents to use for a Genius Result configuration with an NLU trigger condition.

Role required: ais_admin

1. Navigate to **AI Search > Search Query Settings > Genius Results**.
2. Edit the Genius Result configuration that you want to link an NLU model to.
3. In the NLU Model related list, click **Link Existing**.
4. On the form, fill in the fields.

**NLU Model form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Genius Result Configuration</td>
<td>The Genius Result configuration to link the NLU model to. This field is automatically set to the selected Genius Result configuration.</td>
</tr>
<tr>
<td>NLU Model</td>
<td>Existing NLU model to use for the Genius Result configuration's NLU trigger condition.</td>
</tr>
</tbody>
</table>
## ServiceNow DocVersion Now Platform administration

### Field | Description
--- | ---
Intents | List of intents from the NLU model that can trigger the Genius Result configuration when detected in the search query.
Order | Order of evaluation for the NLU model in the context of the Genius Result configuration.
Application | Application scope for the NLU model link. This field is automatically set.

5. Click **Submit**.

The NLU model and its selected intents appear in the NLU Models related list.

For an NLU trigger condition to function, the NLU model must be published. You can verify NLU model status by navigating to **AI Search > Search Query Settings > Search Intents**.

### Result improvement rules

Define rules with configurable trigger conditions to boost, block, or promote search results for specific searches. You can also boost search results for documents matching elements of the user context, such as a user's location or device.

Result improvement rules with boost actions override the default search result order produced by the AI Search machine learning relevancy feature. Rules with block or promote actions override the default result set for a search query.

### Rule structure

A result improvement rule consists of these parts:

- A set of conditions that determine when the rule activates.
- A set of boost, block, or promote actions that determine how the rule modifies the search query's results when activated. The rule can only include actions of a single type, but can include multiple actions of that type.

Rule conditions include the following:

- A date range bounded by start and end dates. The rule can only activate during the specified date range.
- A language. The rule can only activate if this language matches the search query's language.
- Optionally, a set of one or more trigger conditions. Triggers can act on the search query, its intent, or elements of the user context. The rule can only activate if all of its trigger conditions are met.

Rule actions include the following types:

- **Boost**: Increase the relevancy scores for search result records that include specific field values. You can use either of the following options:
  - Boost search result records that include field values matching a dynamically populated value from the user context.
  - Boost search result records that include field values matching a static value that you specify.

- **Block**: Exclude specific records from the search query's results.

- **Promote**: Display specific records at the start of the search query's results.

Each result improvement rule can only perform actions of a single type when activated. You can define multiple actions of the same type for a rule.

Block actions take precedence over promote actions. If two rules block and promote the same record, AI Search excludes the record from the search query's results.
Language dependence

Result improvement rule activation is language-dependent. You specify a language for each result improvement rule. AI Search supports result improvement rules for English, French Canada, French, German, Japanese, and Spanish.

Interaction with other features

The following table describes interactions between result improvement rules with Query triggers and other features that modify the user's search query or its results.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Interaction with result improvement rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lemma and Unicode normalization</td>
<td>A search query term added by lemma or Unicode normalization can trigger a result improvement rule if it matches the rule's Query trigger.</td>
</tr>
<tr>
<td>Stop words</td>
<td>If a search query term that matches a result improvement rule's Query trigger is defined as a stop word, evaluates the rule trigger before removing the stop word from the search query.</td>
</tr>
<tr>
<td>Synonyms</td>
<td>By default, a synonym expansion term can activate a result improvement rule if it matches the rule's Query trigger. You can prevent synonym expansion terms from activating a rule with a Query trigger by clearing the Expand Synonyms For Query Conditions option that appears when you define the Query trigger.</td>
</tr>
<tr>
<td>Typo handling</td>
<td>An auto-corrected search query term can trigger a result improvement rule if it matches the rule's Query trigger.</td>
</tr>
</tbody>
</table>

Create a result improvement rule

Create a rule to boost, block, or promote search results. Specify the conditions that activate your rule and choose the action it performs when activated.

Role required: ais_admin

This topic lists the steps required to configure activation conditions and triggers for a result improvement rule. Additional topics cover steps for configuring boost, block, or promote actions for your rule.

**Note:** Each result improvement rule can only perform actions of a single type when activated. You can define multiple actions of the same type for a rule.

1. Navigate to **AI Search > Search Experience > Search Profiles**.
2. Edit the search profile that you want to add the result improvement rule to.
3. In the Result Improvement Rules related list, click **Create**.
4. On the form, fill in the fields.

**AI Search Result Improvement Rule form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>Unique label for the result improvement rule.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Start Date</td>
<td>System time for first date when the result improvement rule can activate. If left empty, this field is automatically set to the current date.</td>
</tr>
<tr>
<td>End Date</td>
<td>System time for last date when the result improvement rule can activate. After this date, the rule state changes to Expired. If left empty, this field is automatically set to 30 days from the Start Date.</td>
</tr>
<tr>
<td>Activate on all queries</td>
<td>Option to make the result improvement rule activate for every search query.</td>
</tr>
<tr>
<td>Language</td>
<td>Language for the result improvement rule. If you select a language, AI Search only evaluates the result improvement rule for activation if the search query has the same language.</td>
</tr>
<tr>
<td>State</td>
<td>Current state for the result improvement rule.</td>
</tr>
<tr>
<td></td>
<td>• New: The rule has never been published.</td>
</tr>
<tr>
<td></td>
<td>• Draft: The rule is saved with unpublished changes.</td>
</tr>
<tr>
<td></td>
<td>• Published: The rule is saved with all changes published.</td>
</tr>
<tr>
<td></td>
<td>• Expired: The rule cannot activate because its End Date is in the past. Publishing a search profile does not publish expired rules.</td>
</tr>
<tr>
<td>Marked for Deletion</td>
<td>Option indicating that AI Search will delete the result improvement rule the next time you publish the search profile.</td>
</tr>
<tr>
<td>Triggers</td>
<td>Option for enabling synonym expansion for Query condition arguments.</td>
</tr>
<tr>
<td></td>
<td>When expanding Query conditions, AI Search only considers active synonyms that are defined in the same search profile and that have the same language as the result improvement rule.</td>
</tr>
<tr>
<td>Triggers</td>
<td>List of conditions that must be met for the result improvement rule to activate. This field disappears if you select Activate on all queries.</td>
</tr>
</tbody>
</table>

5. Click **Submit**.
   The Actions related list appears.

6. Choose the action that you want the result improvement rule to perform when activated. See the appropriate task topic to configure that action.
   - To increase the relevancy scores of search result records that include specific field values, see **Boost search results using a result improvement rule**.
   - To prevent specific records from appearing in the search results, see **Block search results using a result improvement rule**.
   - To make specific records appear first in the search results, see **Promote search results using a result improvement rule**.
To make new or updated result improvement rule settings take effect, publish the search profile that you edited. For details on publishing a search profile, see Publish a search profile.

Boost search results using a result improvement rule

Configure a result improvement rule to increase the relevancy scores of search results that satisfy a custom condition.

Create your result improvement rule first to define your trigger conditions, then follow these steps to define the action taken when the rule activates. For steps to create a result improvement rule, see Create a result improvement rule.

Role required: ais_admin

1. In the Actions related list, click **Create Boost Action**.
2. On the form, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>Unique label for the boost action.</td>
</tr>
<tr>
<td>Type</td>
<td>Action type. This field is automatically set to Boost Action.</td>
</tr>
<tr>
<td>Application</td>
<td>Application scope for the boost action. This field is automatically set to the name of the current application.</td>
</tr>
<tr>
<td>Order</td>
<td>Order of evaluation for the boost action in the context of the result improvement rule.</td>
</tr>
<tr>
<td>Boost Action</td>
<td></td>
</tr>
<tr>
<td>Boost Type</td>
<td>Type of boost the action applies.</td>
</tr>
<tr>
<td>Indexed Source</td>
<td>Reference to an indexed source. The boost action only applies to records from this indexed source.</td>
</tr>
<tr>
<td>Boost Weight</td>
<td>Numeric value to add to relevancy scores for boosted search results. Positive weights increase result relevancy; negative weights decrease it.</td>
</tr>
</tbody>
</table>

**Note:** Typical boost weights are in the order of 100, 200, 300, and so on.

<table>
<thead>
<tr>
<th>When</th>
<th>Name of a field from the selected search source. This field appears only when you select <strong>Boost by User Context (dynamic)</strong> or <strong>Boost by Field Match (static)</strong> from the <strong>Boost Type</strong> field.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Matches the Searcher's</td>
<td>Dynamically populated value from user context to compare with search result field value. This field appears only when you select <strong>Boost by User Context (dynamic)</strong> from the <strong>Boost Type</strong> field.</td>
</tr>
<tr>
<td>Contains</td>
<td>Static value to compare with search result field value. This field appears only when you select <strong>Boost by Field Match (static)</strong> from the <strong>Boost Type</strong> field.</td>
</tr>
</tbody>
</table>

3. Click **Submit**.

To make new or updated result improvement rule settings take effect, publish the search profile you edited. For details on publishing a search profile, see Publish a search profile.

List of result improvement rule boost types
This list describes the types of search result relevancy boost that you can apply using a result improvement rule.

**Boost action types**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boost All Documents in Search Source</td>
<td>Applies boost to every search result from the selected search source.</td>
</tr>
<tr>
<td>Boost by User Context (dynamic)</td>
<td>Applies boost to search results from the selected search source if they include a value for the selected field that matches a specified element from the dynamically populated user context.</td>
</tr>
<tr>
<td>Boost by Field Match (static)</td>
<td>Applies boost to search results from the selected search source if they include a value for the selected field that matches a specified static value.</td>
</tr>
</tbody>
</table>

Block search results using a result improvement rule
Configure a result improvement rule to prevent specific documents from appearing in results for a search.

Create your result improvement rule first to define your trigger conditions, then follow these steps to define the action taken when the rule activates. For steps to create a result improvement rule, see Create a result improvement rule.

Role required: ais_admin

1. In the Actions related list, click **Block Documents**.
2. In the Select Documents To Block dialog box, search for results that you want to block.
3. To add a search result to the selected results pane, click the plus sign next to it.
4. After selecting all the results that you want to block, click **Add Documents and Close**.

To make new or updated result improvement rule settings take effect, publish the search profile that you edited. For details on publishing a search profile, see Publish a search profile.

Promote search results using a result improvement rule
Configure a result improvement rule to make specific records appear first in results for a search.

Create your result improvement rule first to define your trigger conditions, then follow these steps to define the action taken when the rule activates. For steps to create a result improvement rule, see Create a result improvement rule.

Role required: ais_admin

1. In the Actions related list, click **Promote Documents**.
2. In the Select Documents To Promote dialog box, search for the results that you want to promote.
3. To add a search result to the selected results pane, click the plus sign next to it.
4. After selecting all the results that you want to promote, click **Add Documents and Close**.

To make new or updated result improvement rule settings take effect, publish the search profile that you edited. For details on publishing a search profile, see Publish a search profile.

**Search application configurations**
Define search application configurations that specify AI Search as the search engine for supported Now Platform applications. Select a search experience for the application and configure its search result display and refinement settings.

AI Search includes default search application configurations for use in the following Now Platform applications:

- Employee Service Center (ESC) Portal
- Service Portal
Virtual Agent

You can modify these default configurations, or create and configure your own search application configurations with AI Search specified as the search engine.

For details on enabling AI Search and specifying search application configurations in supported applications, see Enabling and configuring AI Search in Now Platform applications.

Create a search application configuration for AI Search
Create a search application configuration to specify AI Search as the search engine for a Now Platform application. Select a search profile for the application to use. Configure the application's settings for refinement and display of search results.

Role required: search_application_admin

1. Navigate to AI Search > Search Experience > Search Applications.
2. Click New.
3. On the form, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name for the search application configuration.</td>
</tr>
<tr>
<td>Search Engine</td>
<td>Search engine to use in the Now Platform search application that links to the search application configuration. Supported values:</td>
</tr>
<tr>
<td></td>
<td>• <strong>AI Search</strong>: Use AI Search as the search engine for the application. Select this engine if your search application has the Enable AI Search option enabled.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Zing</strong>: Use the Zing text indexing and search engine as the search engine for the application. Select this engine if your search application has the Enable AI Search option disabled, or if it lacks this option.</td>
</tr>
<tr>
<td>Search Profile</td>
<td>Search profile to use for searches in the application. This field appears only when you select AI Search from the Search Engine field.</td>
</tr>
<tr>
<td>Search Results Limit</td>
<td>Maximum number of search results the application should display on each search results page. This limit also specifies the minimum number of search results each query should return. When a search query returns less than this number of results, AI Search attempts to broaden the result set by automatically resubmitting the query with modified parameters. For more details on query resubmission, see Automatic search query resubmission.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Genius Results Limit</td>
<td>Maximum number of Genius Result answer cards the application should display on the search results page. This field appears only when you select AI Search from the Search Engine field.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Genius Results return a maximum of 3 answer cards per search query. If you set this limit to 4 or more, AI Search still displays a maximum of 3 answer cards.</td>
</tr>
<tr>
<td>Enable Typo Handling</td>
<td>Option to auto-correct search query terms to match terms found in the search profile’s typo handling dictionary. This field appears only when you select AI Search from the Search Engine field.</td>
</tr>
<tr>
<td></td>
<td>For more details on typo handling auto-correction configuration and behavior, see Typo handling.</td>
</tr>
</tbody>
</table>

4. Click Submit.

The new search application configuration record appears in the Search Application Configurations list.

To use your new search application configuration, select it in the configuration for a Now Platform application that supports AI Search. For more information on these Now Platform applications, see Enabling and configuring AI Search in Now Platform applications.

Enable or disable hit-highlighting for an AI Search application

Specify whether your search application should highlight matching search terms when displaying search query results.

Role required: search_application_admin

1. Navigate to AI Search > Search Experience > Search Applications.
2. Edit the search application configuration that you want to change the hit-highlighting setting for.
   
   **Note:** The search application configuration must have AI Search selected as its search engine. Hit-highlighting is only available when using AI Search.

3. On the Search Application Configuration form, if the Enable Hit-Highlighting field is not displayed, follow these steps to add it:
   a) Click the form context menu icon
      
      ![Form Context Menu Icon](image)
      
      and select Configure > Form Layout.
   b) Move Enable Hit-Highlighting to the Selected list.
   c) Click Save.

4. Select or deselect the Enable Hit-Highlighting option.
5. Click Update.
Create a facet in an AI Search application configuration
Create facets to help your users refine their searches using categories dynamically generated from the current search results.

Role required: search_application_admin

1. Navigate to **AI Search > Search Experience > Search Applications**.
2. Edit the search application configuration that you want to configure a facet for.
3. In the Facets related list, click **New**.
4. On the form, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name for the facet.</td>
</tr>
<tr>
<td>Label</td>
<td>Label to display for the facet in the search application.</td>
</tr>
<tr>
<td>Facet Field</td>
<td>Qualified name of the AI Search index field that the facet uses to categorize search results for refinement. Specify this field name in <code>[table_name].[field_name]</code> format.</td>
</tr>
<tr>
<td>Facet Value Limit</td>
<td>Maximum number of distinct field values to display for the facet.</td>
</tr>
<tr>
<td>Order</td>
<td>Order of appearance for the facet in the context of the search application configuration.</td>
</tr>
<tr>
<td>Active</td>
<td>Option to activate the facet for the application.</td>
</tr>
</tbody>
</table>

5. Click **Submit**.

The new facet appears in the Facets related list.

Configure navigation tabs in an AI Search application configuration
Define settings for navigation tabs in a search application configuration. Users of the application can select navigation tabs to refine their search query results by search source.

Role required: search_application_admin

AI Search automatically defines navigation tabs for search application configurations. Each tab is tied to a search source linked to the search application configuration's search profile. You cannot create or delete these navigation tabs.

Follow these steps to configure display settings for navigation tabs in your search application configuration.

1. Navigate to **AI Search > Search Experience > Search Applications**.
2. Edit the search application configuration that you want to configure navigation tabs for.
3. In the Navigation Tabs related list, edit the navigation tab that you want to configure.
4. On the form, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name for the navigation tab. This field is set by default to the name of the originating search source. Changing the name does not affect the navigation tab's filtering behavior.</td>
</tr>
<tr>
<td>Active</td>
<td>Option to enable the navigation tab. Inactive navigation tabs are not displayed.</td>
</tr>
<tr>
<td>Order</td>
<td>Order of appearance for the navigation tab in the context of the search application configuration.</td>
</tr>
<tr>
<td>Label</td>
<td>Label to display for the navigation tab in the search application.</td>
</tr>
<tr>
<td>Search Context Config</td>
<td>Search application configuration for the navigation tab.</td>
</tr>
</tbody>
</table>

5. Click Update.

The navigation tab appears with updated settings in the Navigation Tabs related list.

Auto-complete suggestions in AI Search applications

Automatically display intelligent suggestions in your search application's input field, helping users formulate their searches or jump directly to relevant results. Suggestions include popular queries, recent queries from the user's personal history, and popular search results.

When you create a new search application configuration, AI Search automatically populates it with auto-complete suggestion types. The settings for these suggestion types control the appearance of auto-complete suggestions when users interact with its input field.

Each auto-complete suggestion type includes default settings that you can configure to suit your application's needs.

You can remove an unwanted suggestion type from your search application configuration. If you need to restore a removed suggestion type, you can relink it to your search application configuration. You can only link one auto-complete suggestion source of each type to any given search application configuration.

Auto-complete suggestions are generated by the Search Suggestions application. For full details on configuration and use of the Search Suggestions application, see Search Suggestions.

List of auto-complete suggestion types for AI Search

AI Search provides auto-complete suggestions derived from popular and recent search queries and frequently selected search results.

Auto-complete displays the following types of suggestions in the search application's input field:

**Popular Searches**
Displays search queries commonly submitted by all users of the search application as suggestions.

**Recent Searches**
Displays search queries drawn from the user's recent personal search history for the search application as suggestions.

**Suggested Queries**
Displays a mixture of recent and popular search queries as suggestions.

**Suggested Results**
Displays search results that the user has selected from previous search queries as suggestions.
Configure an auto-complete suggestion type in an AI Search application configuration
Modify default settings for display of auto-complete suggestions of a selected type in your search application's input field.

Role required: search_application_admin

When you define a new search application configuration, AI Search automatically populates it with auto-complete suggestion types. You can alter the default settings for these auto-complete suggestion types.

1. Navigate to **AI Search > Search Experience > Search Applications**.
2. Edit the search application configuration that contains the auto-complete suggestion type that you want to modify.
3. In the Autocomplete Suggestions related list, edit the auto-complete suggestion type that you want to modify settings for.
4. On the form, fill in the fields.

**Suggestion Reader Group form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suggestion Type</td>
<td>Application-specific name for the auto-complete suggestion type. This field is automatically set.</td>
</tr>
<tr>
<td>Section Header</td>
<td>Header displayed in the application search field for auto-complete suggestions of this type.</td>
</tr>
<tr>
<td>Application</td>
<td>Application scope for the auto-complete suggestion type. This field is automatically set.</td>
</tr>
<tr>
<td>Order</td>
<td>Order of appearance in the application search field for the section containing auto-complete suggestions of this type.</td>
</tr>
<tr>
<td>Suggestion Limit</td>
<td>Maximum number of auto-complete suggestions of this type that the application should display in the search field.</td>
</tr>
<tr>
<td>Click-in Mode</td>
<td>Option to control the display of the section containing auto-complete suggestions of this type.</td>
</tr>
<tr>
<td></td>
<td>• If selected, auto-complete suggestions of this type are displayed when the user first clicks in the empty application search field.</td>
</tr>
<tr>
<td></td>
<td>• If deselected, auto-complete suggestions of this type are displayed as the user enters search query terms into the application search field.</td>
</tr>
</tbody>
</table>

5. Click **Update**.

The updated settings for the auto-complete suggestion type appear in the search application configuration's Autocomplete Suggestions related list.

Remove an auto-complete suggestion type from an AI Search application configuration
Disable the display of auto-complete suggestions of a selected type in your search application's input field.

Role required: search_application_admin

When you define a search application configuration, AI Search automatically populates it with auto-complete suggestion types. You can remove unwanted auto-complete suggestion types from the search application configuration.

1. Navigate to **AI Search > Search Experience > Search Applications**.
2. Edit the search application configuration that contains the auto-complete suggestion type you want to remove.
3. In the Autocomplete Suggestions related list, edit the auto-complete suggestion type that you want to remove.

4. On the Suggestion Reader Group form, click Remove from Search Application.

The selected auto-complete suggestion type no longer appears in the search application configuration's Autocomplete Suggestions related list.

Relink an auto-complete suggestion type to an AI Search application configuration

Re-enable the display of auto-complete suggestions of a selected type in your search application's input field.

Role required: search_application_admin

When you define a search application configuration, AI Search automatically populates it with auto-complete suggestion types. If you removed one of these auto-complete suggestion types from the search application configuration, you can relink it.

**Note:** You can only link one auto-complete suggestion source of each type to any given search application configuration.

1. Navigate to AI Search > Search Experience > Search Applications.
2. Edit the search application configuration that you want to relink the auto-complete suggestion type to.
3. In the Autocomplete Suggestions related list, click Add Existing.
4. In the Suggestion Reader Groups list, edit the auto-complete suggestion type that you want to relink to your search application configuration.
5. On the Suggestion Reader Group form, enter or look up the search application configuration name in the Search Application field.
6. Click Update.

The selected auto-complete suggestion type appears in the search application configuration's Autocomplete Suggestions related list.

**Using search scripted post-processors in AI Search application configurations**

Use scripted post-processors to modify search result records for display in a search application.

For example, a search scripted post-processor can modify search result date or currency field values to display in the user's regional formats.

Create a search scripted post-processor

Define a script to post-process AI Search search results before displaying them to the user.

Role required: search_application_admin

1. In the filter navigator, enter sys_search_scripted_processor.list and press Enter.
2. In the Search Scripted Post-processors table, click New.
3. On the form, fill in the fields.

**Search Scripted Post-processor form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Option to activate the search script post-processor.</td>
</tr>
<tr>
<td>Name</td>
<td>Name for the search script post-processor.</td>
</tr>
<tr>
<td>Application</td>
<td>Application scope for the search script post-processor.</td>
</tr>
<tr>
<td></td>
<td>This field is automatically set.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Type                     | Type of record the search script post-processor operates on.  
                            | Valid values:  
                            | • Genius Result: Script operates on a Genius Result answer record.  
                            | • Search Result: Script operates on a search result record.                                                                     |
| Post processing script   | Server-side script function that takes a record object as its parameter. When the search scripted post-processor is linked to a search application configuration, search results reflect changes made to the record object in this function. |

**Note:** The UI displays an overview of API methods usable in the post-processing script function.

4. Click **Submit**.

The new search scripted post-processor appears in the Search Scripted Post-processors table.

To make your new search scripted post-processor take effect, link it to the search application configuration for the application whose results you want to post-process.

**Link a search scripted post-processor to an AI Search application configuration**

Link a search scripted post-processor to an AI Search application configuration. The search application executes the linked script for each search result before displaying it to the user.

Role required: search_application_admin

You must have already created the search script post-processor that you want to link to the search application configuration.

1. Navigate to **AI Search > Search Experience > Search Applications.**
2. Edit the search application configuration that you want to link a search scripted post-processor to.
3. In the Search Scripted Post-processors related list, click **New.**
4. On the Search Scripted Post-processors form, click the reference lookup icon (🔍) for the **Search scripted processor** field and select the search scripted post-processor that you want to link to the search application configuration.

5. Click **Submit**.

The new search scripted post-processor appears in the Search Scripted Post-processors related list.

**Enabling and configuring AI Search in Now Platform applications**

Configure and use the AI Search engine in the , , and  applications.

For each supported Now Platform application that you want to use AI Search in, define a search application configuration and specify AI Search as the search engine. To learn more about search application configurations, see **Search application configurations.**

Some applications support additional configuration for AI Search, as described in the following sections.
Service Portal

**Service Portal** is a portal framework that enables administrators to build a mobile-friendly self-service experience for users. It interacts with parts of the Now Platform, so users can access specific platform features using Service Portal.

For details on enabling and using AI Search as the Service Portal search engine, see Enable and configure AI Search in Service Portal.

Now Mobile

Enable your users to submit incidents and requests, manage tasks, and access company resources from anywhere using the **Now Mobile** app.

For details on configuring and using AI Search as the Now Mobile search engine, see AI Search in mobile.

Virtual Agent

**Virtual Agent** is a platform for providing user assistance through conversations within a messaging interface. Use Virtual Agent to design and build automated conversations that help your users quickly obtain information, make decisions, and perform common work tasks.

For information on how Virtual Agent uses AI Search, see Virtual Agent integration with AI Search.

Domain separation and AI Search

Domain separation is unsupported for the AI Search application tables, but user search queries respect domain restrictions from indexed Now Platform table records. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can control several aspects of this separation, including which users can see and access data.

**Note:** Refer to the Overview and following sections for details on how AI Search search queries respect domain settings from indexed records.

Support level: No support

- The domain field may exist on data tables but there is no business logic to manage the data.
- This level is not considered domain-separated.

For more information, see Application support for domain separation.

Overview

AI Search enables users to index and search content from records in Now Platform tables. The AI Search application tables and properties do not support domain separation, but user search queries respect domain settings from indexed content as described in the following sections.

Domain separation in indexed content and search queries

When indexing searchable content from a Now Platform table, AI Search stores the `sys_domain` field values for records on the source table and referenced tables.
If domain separation is enabled, AI Search applies a filter for the current session domain to every search query. This filter excludes records that are not visible in the session domain. Only records visible in the session domain appear as search query results.

For child tables that have the domain_master attribute set, both indexing and search use the appropriate reference field to derive the child record domain from a referenced parent record.

Restrictions apply to referenced records in search queries, as summarized in the following table.

<table>
<thead>
<tr>
<th>Condition</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Referenced record is not visible in current session domain</td>
<td>• Search queries do not match content from the referenced record</td>
</tr>
<tr>
<td></td>
<td>• Filtering on the reference field has no effect on search results</td>
</tr>
<tr>
<td></td>
<td>• Faceting on the reference field has no effect</td>
</tr>
<tr>
<td>Referenced record domain differs from parent record domain</td>
<td>Search result records do not display the reference field</td>
</tr>
</tbody>
</table>

### Indexing changes to record domains

AI Search automatically updates indexed domains for records in tables configured as indexed sources.

AI Search does not automatically update indexed domains for referenced tables. You can update the indexed domain for a referenced table in either of the following ways.

<table>
<thead>
<tr>
<th>Use case</th>
<th>Action</th>
</tr>
</thead>
</table>
| Perform a one-time update of domain field values for a referenced table | Perform a full table reindex for the indexed source that includes the affected table.  
For details on this procedure, see [Perform a full table index or reindex for a single indexed source](#). |
| Enable automatic updating of domain field values for a referenced table | Create a dot_walk_fields field setting for the reference field, specifying the sys_domain,sys_domain_path domain fields as the attribute value.  
For full steps for this task, see [Enable automatic domain updates for a referenced table](#). |

**Enable automatic domain updates for a referenced table**

Configure a field setting to automatically index domain field value updates for records from a referenced table.

Role required: ais_admin

This topic provides steps for configuring a dot_walk_fields field setting to enable automatic indexing of domain field values for records in referenced tables. For more general instructions on defining field settings, see [Create a field setting for an indexed source](#).

1. Navigate to **AI Search > AI Search Index > Indexed Sources**.
2. Edit the indexed source that you want to define a field setting for.
3. In the Field Settings & Mapping related list, click **New**.
4. On the Field Setting form, enter the following field values.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute</td>
<td>dot_walk_fields</td>
</tr>
<tr>
<td>Field</td>
<td>&lt;reference field&gt;</td>
</tr>
<tr>
<td>Value</td>
<td>sys_domain.sys_domain_path</td>
</tr>
</tbody>
</table>

5. Click Submit.

The new **dot_walk_fields** field setting appears in the Field Settings & Mapping related list.

To make the new **dot_walk_fields** attribute take effect, perform a full table reindex for the indexed source. For details on this procedure, see Perform a full table index or reindex for a single indexed source.

**Indexing and searching external content in AI Search**

Make content from external data sources searchable in Now Platform applications that support AI Search.

To enable indexing of content from external data sources, you must purchase a subscription for the External Content plugin (com.glide.ais.external_content) and activate it.

Next, you must create and configure an external content schema table. This table does not store data in the database. Instead, its columns serve as a map of AI Search index fields to populate when you index content from the external data source.

Finally, you must create an indexed source for the content schema table and derive search sources from it. Link these search sources to search profiles normally.

After defining the indexed source, you can use the External Content Ingestion REST API to index searchable content for the external data source's documents:

- Feed external data source documents to the AI Search index using the `ingestDocuments` API endpoint.
- Upload external data source document binary content to AI Search using the `storeContent` API endpoint. You can link this uploaded binary content stream to a document fed via the `ingestDocuments` endpoint.
- Delete external data source documents from the AI Search index using the `deleteDocument` and `deleteByQuery` API endpoints.

Once documents from the external data source are indexed, your users can search for them just as they would for records indexed from Now Platform tables.

**Using an external content schema table for multiple external data sources**

You can use the same external content schema table for multiple external data sources. To avoid data loss, the external data sources must satisfy these conditions.

- All documents in the external data sources must include the same fields, matching the columns defined in the content schema table.
- Every document in the external data sources must have a unique identifier so that documents do not overwrite one another in the AI Search index.

If the external data sources cannot satisfy these conditions, create a separate external content schema table for each data source.
Content security for external content

In the release, does not index security settings for external content. As a result, all users can view all indexed external records as search results.

For more information on AI Search content security, see Content security in AI Search.

Activate the External Content for AI Search plugin

The External Content for plugin (com.glide.ais.external_content) provides support for indexing searchable content from records in external data sources.

You must purchase a paid subscription before activating the plugin. For details on purchasing a paid subscription for a plugin, see ServiceNow plugins.

Role required: admin

1. Navigate to System Applications > All Available Applications > All.
2. Find the plugin using the filter criteria and search bar.
   You can search for the plugin by its name or ID. If you cannot find a plugin, you might have to request it from ServiceNow personnel. For more information, see Request a plugin.
3. Click Install, and then in the Activate Plugin dialog box, click Activate.

   Note: When domain separation and delegated admin are enabled in an instance, the administrative user must be in the global domain. Otherwise, the following error appears: Application installation is unavailable because another operation is running: Plugin Activation for <plugin name>.

Create an external content schema table

Define a schema table with columns corresponding to fields on records from an external data source. AI Search uses the schema when indexing content from the external data source.

Role required: ais_admin

1. Navigate to AI Search > External Content > Create Schema.
2. Enter a name for your new external source schema table.
3. Click Submit.
   The new external content schema table opens in list view.
4. Optional: If you need to define additional field mappings for records from the external data source, add a new column for each field by following these steps.
   a) In the Columns related list, click New.
   b) On the Dictionary Entry form, fill in the fields. For descriptions of these fields, see Dictionary entry form.

      Note: When filling in the Type field, select String, Date, Date/Time, or Integer. AI Search only supports these column types on external content schema tables.

   c) Click Submit.
5. If you modified the default column set, click Update to save your changes.

Record the new schema table’s name. When you index or delete records associated with this content schema using endpoints from the External Content Ingestion REST API, you must specify the schema table name as a path parameter.
Components installed with External Content for AI Search
When you activate the External Content for plugin (com.glide.ais.external_content), the system creates a new virtual table.

Tables installed

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI Search External Search Content [v_ais_external_search_content]</td>
<td>Stores the base set of field mapping columns for inclusion in external content schema tables.</td>
</tr>
</tbody>
</table>

Note: All user-created external content schema tables extend this table.

Integrating AI Search into your instance or application
You can create and configure search profiles to use with AI Search Assist.

AI Search Assist integration
AI Search Assist uses AI Search to:
- Create a search profile that can link to a portal
- Add Knowledge Base articles or Catalog items

Search components in UI Builder
You can add search components to a custom-built application in UI Builder. These components include:
- Search facets
- Search input
- Search results
- Tab filter

EVAM integration
Entity View Action Mapper (EVAM) is an application that standardizes how different data sources display in cards and lists.
EVAM enables you to show information as a card grid view or as a list view. Users can page through large data sets of search results and see different views based on filtering.
AI Search Assist

AI Search Assist uses AI Search functionality to fetch the most relevant set of search results for users. AI Search Assist displays related results within a record producer and can be used instead of Contextual Search.

Overview

AI Search Assist can help a user find the most relevant items in a search on your portal. For example:

- A user, creating an Incident via the Service Portal, can see related catalog items that the user can order. The user can also view related Knowledge articles to assist them to resolve the issue on their own without involving the service desk.

AI Search Assist helps with incident deflection for the following areas:

- Incident record producers: Deflecting incidents by helping end users resolve issues before they raise an incident.

AI Search Assist supports ServiceNow mobile.

Activation information

The AI Search Assist plugin (com.snc.ai_search_assist) is a Now Platform application that is activated by default when AI Search is active.

Configure AI Search Assist for a record producer

You can configure different components of AI Search Assist.

Role required: admin or aisa_admin

AI Search Assist is a Service Portal widget used with a record producer configuration.

Note: If both AI Search Assist and Contextual Search are configured for the same record producer, see the Results at the end of this task for how to control which one is displayed.

1. Navigate to AI Search > AI Search Assist > Record Producer Configuration.
2. Click New and fill in the form to create a configuration for search results.

Record Producer Configuration form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Title of the record producer configuration. For example, Search Results.</td>
</tr>
<tr>
<td>Results per page</td>
<td>Number of search results to display per page.</td>
</tr>
<tr>
<td>Allow expand/collapse</td>
<td>Option to allow users to expand or collapse search results in this record producer configuration.</td>
</tr>
<tr>
<td>Active</td>
<td>Option to make this record producer configuration active for your instance.</td>
</tr>
<tr>
<td>Application</td>
<td>Application scope for this record producer configuration.</td>
</tr>
</tbody>
</table>
3. On the **Search application information** tab, select a Search application configuration. You can choose from a list of pre-defined configurations for specific features. For example, **[AI Search Assist] - Incident Deflection**.

4. On the **Record producer information** tab, select a Record producer and Search variable. For example, **Service Category Request** as a record producer can have a search variable of **Category name**.

5. Optional: To adjust the visibility of your card or detail view, click **Show UI Actions** under the new Record Producer Configuration record’s related links. **AI Search Assist UI actions** can hide from view using a simple condition or advanced condition via a script.
6. Click **Submit**.

AI Search Assist is active. If Contextual Search has been configured for the same record producer, and is showing results instead of AI Search Assist, check the following conditions:

- The **Enable AI Search** flag on the Portal (sp_portal) is active
- The AI Search Assist record configuration is active
- The AI Search Profile is active and published
- The record producer variable for AI Search Assist is created for the associated record producer and the variable is active

If these conditions are not all met, then Contextual Search is the fallback for the same record producer to make sure you see related search results.

**AI Search Assist admin role**

Grant users the AI Search Assist admin role [aisa_admin] so they can configure and manage AI Search Assist settings.

### AI Search Assist admin role

<table>
<thead>
<tr>
<th>Roles</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI Search Assistant administrator [aisa_admin]</td>
<td>Users with the aisa_admin role can do the following:</td>
</tr>
<tr>
<td></td>
<td>• Manage AI Search Assist on record producers, including the associated UI actions</td>
</tr>
<tr>
<td></td>
<td>• Add a variable to a record producer</td>
</tr>
<tr>
<td></td>
<td>• Administer AI Search capability</td>
</tr>
</tbody>
</table>

**AI Search Assist properties**

The AI Search Assist properties determine when searching begins based on characters entered and the time that has elapsed. These properties reduce the impact of searches for systems with many Catalog Items or Knowledge articles.

### AI Search Assist properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.snc.ai_search_assist.min_length</td>
<td>The minimum number of characters entered before a search initiates. The default is 3.</td>
</tr>
</tbody>
</table>
| com.snc.ai_search_assist.wait_time     | The time elapsed after the user finishes entering characters in the search field before the search begins. | 💡 **Note:** If you set the time to `-1`, the search begins when the user leaves the search field. This behavior is known as 'Search on tab'.

**Domain separation and AI Search Assist**

Domain separation is supported for AI Search Assist. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can control several aspects of this separation, including which users can see and access data.
Overview

The goal of AI Search Assist is to give a Service Portal record producer AI Search capabilities, which improve search results over time. Domain separation is enabled in AI Search Assist.

How domain separation works in AI Search Assist

Domain separation for AI Search Assist is set in the record producer configuration. A related link for each record producer configuration enables you to expand or collapse the domain scope. If you expand the domain scope, any child domain record producer configurations can override a global or parent domain record configuration.

Using AI Search

See how AI Search displays search results, refinement filter options, and Genius Result answers. Learn how to search using the AI Search query language. Understand when and how AI Search automatically resubmits queries.

Viewing search results

Learn about the components that AI Search uses to display results for search queries.

Search result page elements

The layout and appearance of AI Search UI elements varies from application to application. This example shows the elements as they might appear on a Service Portal search results page.
Sample search result screen
## Search result screen elements

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Search input field</td>
<td>Displays the search query that produced the listed search results. You can modify this search query and search again to view different results.</td>
</tr>
<tr>
<td>2. Navigation tab filters</td>
<td>Displays static filter options for refining search results by source. To view only search results from a single source, click the source name. Click <strong>All</strong> to remove the navigation tab filter.</td>
</tr>
<tr>
<td>3. Facet filters</td>
<td>Displays dynamic filter options for refining search results by field value. To expand or collapse a facet, click the + (plus) or - (minus) symbol by its name. To view only search results that contain a specific field value, select the field value in the facet. Deselect the field value to remove the facet filter.</td>
</tr>
<tr>
<td>4. Genius Result answer cards</td>
<td>Display the best answers for the search query along with actions you can take directly from each card. <strong>Note:</strong> Genius Result answer cards may not appear for all search queries.</td>
</tr>
<tr>
<td>5. Search results</td>
<td>Displays the icon, summary field values, title, and text snippet for each search result. Click a result to view its source record in full. <strong>Note:</strong> When hit-highlighting is enabled for the search application, AI Search highlights search query terms found in search result titles and text snippets.</td>
</tr>
</tbody>
</table>

## Auto-correction message

When AI Search auto-corrects a misspelled search query term, a **Showing results for <corrected_term>** message appears above the search results list.
**Auto-correction message elements**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6. Typo handling auto-correction message and link</td>
<td>Displays the auto-corrected query term used for the search. To repeat the search using your original search query term, click the <strong>Search instead for &lt;original_term&gt;</strong> link that appears below the message.</td>
</tr>
</tbody>
</table>

**AI Search query language**

Learn how to construct search queries using terms, phrases, and AI Search query operators.

**Search query terms and phrases**

Specify terms and quoted phrases in the search query to find records that contain the same words or phrases.

<table>
<thead>
<tr>
<th>Search query terms</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>conference room</td>
<td>Conjunctive multi-term search. Finds records that contain both conference and room (an intersection of sets). The search terms can appear in any order or proximity in the record and may appear in different fields.</td>
</tr>
</tbody>
</table>

**Note:** If you set the **Boolean search operator to use when a search query includes multiple terms** (glide.ais.query.search_operator) system property to **OR query**, this search finds records that contain either conference or room (a union of sets).

| "conference room" | Quoted phrase search. Finds records that contain conference followed immediately by room. The search terms must appear in this order and in the same field. |

**Note:** Quoting a phrase does not disable linguistic features (such as normalization, synonym expansion, and stop word removal) or wildcard operators. For example, a search for the quoted phrase "email acc*" expands the wildcard operator normally to find records that contain email account and email access.

Search ignores letter case for search query terms and phrases. For example, searching for PIN finds records containing PIN and pin.
### Boolean search operators

Separate query terms and phrases with Boolean operators to override the default matching logic for the search query.

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OR</td>
<td>Boolean disjunction operator. Finds records that contain any of the terms or phrases separated by OR. For example, searching for &quot;conference room&quot; OR suite finds records that contain the phrase conference room and records that contain the term suite.</td>
</tr>
<tr>
<td>hyphen (−)</td>
<td>Boolean negation operator. Excludes records containing the term or phrase that immediately follows the hyphen. For example, searching for email -&quot;email signature&quot; finds records that contain the term email but do not contain the phrase email signature.</td>
</tr>
</tbody>
</table>

**Note:** If you set the **Boolean search operator to use when a search query includes multiple terms** (glide.ais.query.search_operator) system property to **OR query**, this operator has no effect because search already treats all query terms and phrases as though separated by the OR operator.

### Wildcard matching operators

Use wildcard operators to find records that contain indexed terms matching a wildcard pattern.

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%</td>
<td>Single-character wildcard operator. Include % in a search query term to match any one character in an indexed term. For example, searching for the%e finds records containing theme, there, or these.</td>
</tr>
</tbody>
</table>

**Note:** The % operator must follow a string of three or more non-wildcard characters. Without this prefix, the search query finds no records.
ServiceNow    DocVersion    Now Platform administration

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>String wildcard operator. Include * in a search query term to match any string of zero or more characters in an indexed term. For example, searching for acc* finds records containing access, account, accrue, accumulate, accuracy, and so on.</td>
</tr>
<tr>
<td>***</td>
<td>Universal wildcard operator. Specify *** as a search query term to find all indexed terms and thus all records.</td>
</tr>
</tbody>
</table>

**Automatic search query resubmission**

When a search query returns too few results, AI Search automatically modifies and resubmits it with the goal of returning at least the desired number of results.

Search administrators configure the minimum number of desired results per search query using the **Search Results Limit** field in search application configurations. For more details, see Create a search application configuration for AI Search.

**AND-to-OR search query resubmission**

When a search query with conjunctive terms or phrases returns insufficient results, AI Search resubmits it with the default Boolean operator changed from AND to OR and displays results for the modified query.

For example, if a query for hotel "conference room" suite matches no results, AI Search resubmits it as hotel OR "conference room" OR suite. This less-restrictive query may match more results than the original query.

**Note:** If you set the **Boolean search operator to use when a search query includes multiple terms** (glide.ais.query.search_operator) system property to **OR query**, AI Search does not resubmit search queries in this way because the initial search already treats all query terms and phrases as though separated by the OR operator.

When automatically resubmitting a search query in this way, AI Search adds a minimum match count restriction to the OR expression. The modified query only returns results that match at least half (rounded up) of the terms separated by OR operators. This restriction improves query performance and provides more relevant results.

For example, suppose a search query for laptop can't access wi-fi network returns no results. AI Search automatically resubmits the query as laptop OR can't OR access OR wi-fi OR network. Only records that match at least three of the five query terms appear as results for the resubmitted search.

**Conditions for automatic search query resubmission**

Automatic search query resubmission ignores search queries that meet any of the following conditions.

- The original search query only includes a single term.
- The original search query includes 8 or more terms and returns at least one search result.
Administering AI Search

Learn how AI Search features and behavior affect indexing and search. Gain insight into AI Search behavior by reviewing log messages, ingestion history for indexed sources, and session debugging messages.

AI Search and performance testing

Understand how the AI Search topology affects performance testing on instances created with System Clone.

**Warning:**

Be careful when testing AI Search performance in cloned non-production instances. The same dedicated AI Search nodes handle search query traffic from all of your instances. As a result, search queries on non-production instances may impact search query performance in your production instance.

Lemma and Unicode normalization

AI Search normalizes inflected words and Unicode glyphs during indexing and at search query time. Normalization improves search recall and enables users to find content with variant forms of their search query terms.

Normalization features are automatically enabled and are not configurable.

Lemma normalization

Many languages include inflected forms of terms, such as plural nouns or verb tenses. AI Search normalizes inflected terms found in indexed content and search queries. Normalization enables matching based on a root form, such as the singular for a plural noun or the base form for a conjugated verb. This root form is called a lemma, and this process is referred to as lemma normalization.

For example, when a source record includes the conjugated verb *selling*, AI Search expands the indexed term to include the lemma form *sell* in addition to *selling*. When a user searches for the past-tense conjugated form *sold*, AI Search expands the search query term to include the lemma form *sell* as well as *sold*. Because the indexed term and the search query term include matching forms, the user's search returns the *selling* record as a result.

AI Search supports language-specific lemma normalization for English, French Canada, French, German, Japanese, and Spanish.

As part of lemma normalization for German, AI Search splits compound words into their components. For example, when indexing a record that contains the compound word *Humanressourcen*, AI Search indexes the component terms *Human* and *ressourcen* in addition to the compound term.

Unicode normalization

AI Search performs Unicode normalization on indexed terms and search query terms. This normalization makes alphabetical Unicode glyphs searchable using their nearest equivalent characters.

For example, when indexing a record containing the term *resumé*, AI Search expands the term to also include the non-accented form *resume*. This record appears as a search result when users search for either *resume* or *resumé*.

Unicode normalization includes NFKD (compatibility decomposition) and NFKC (compatibility composition) stages. For more information on these normalization forms, see the Unicode Standard Annex #15, https://www.unicode.org/reports/tr15/.
Interaction with other features

The following table describes interactions between normalization and other features that modify search queries or results.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Interaction with lemma and Unicode normalization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Genius Results</td>
<td>Search query terms added by lemma or Unicode normalization cannot trigger Genius Result configurations with Term trigger conditions.</td>
</tr>
<tr>
<td>Result improvement rules</td>
<td>A search query term added by lemma or Unicode normalization can trigger a result improvement rule if it matches the rule's Query trigger.</td>
</tr>
<tr>
<td>Stop words</td>
<td>If a search query term is defined as a stop word, removes the term without normalizing it.</td>
</tr>
<tr>
<td>Synonyms</td>
<td>If a search query term is defined as a synonym, does not normalize it.</td>
</tr>
<tr>
<td>Typo handling</td>
<td>Performs lemma and Unicode normalization on auto-corrected search query terms.</td>
</tr>
</tbody>
</table>

Internationalization support for AI Search

AI Search supports search in all languages offered by the Now Platform. Search query linguistic features support English, French Canada, French, German, Japanese, and Spanish.

Internationalization support is automatically enabled and is not configurable.

Indexing and search query behavior in supported languages

When indexing searchable content, AI Search preserves the language specified for the source table record. If a record has no specified language, AI Search uses heuristics to detect its language.

At query time, AI Search inherits the language from the Now Platform language context. Only records with this language are returned as search results.

These language settings determine how AI Search tokenizes the text of indexed content or search query terms. When the language for the indexed content matches the search language context, the tokenization settings match and search returns results.

Search query linguistic features

The following search query linguistic features are language-dependent and supported only for the listed languages.
# Search feature language dependence

<table>
<thead>
<tr>
<th>Feature</th>
<th>Language dependence and supported languages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Genius Results</td>
<td>AI Search only evaluates Genius Results with NLU triggers if the linked NLU model has the same language as the search query. Supported languages: English.</td>
</tr>
<tr>
<td>Lemma and Unicode normalization</td>
<td>AI Search performs language-specific lemma normalization for search query terms from supported languages. Supported languages: English, French Canada, French, German, Japanese, and Spanish. For German, AI Search performs term decompounding as part of lemma normalization. AI Search performs Unicode normalization for all search query terms.</td>
</tr>
<tr>
<td>Result improvement rules</td>
<td>AI Search only evaluates result improvement rules that have the same language as the search query and rules that have no language specified. Supported languages: English, French Canada, French, German, Japanese, and Spanish.</td>
</tr>
<tr>
<td>Stop words</td>
<td>AI Search only considers stop words from dictionaries that have the same language as the search query. Supported languages: English, French Canada, French, German, Japanese, and Spanish.</td>
</tr>
<tr>
<td>Synonyms</td>
<td>AI Search only considers synonyms from dictionaries that have the same language as the search query. Supported languages: English, French Canada, French, German, Japanese, and Spanish.</td>
</tr>
<tr>
<td>Typo handling</td>
<td>AI Search derives a separate list of auto-correction terms for each supported language found in search source indexed content. Auto-correction only replaces search query terms with terms from the list that has the same language as the search query. Supported languages: English, French Canada, French, German, and Spanish. Japanese is not supported.</td>
</tr>
</tbody>
</table>

## Machine learning relevancy in AI Search

AI Search displays the most relevant search results for a query first. Machine learning automatically tunes search result relevancy scoring for search experiences based on aggregated user interactions.

Machine learning relevancy is automatically enabled and is not configurable.
Relevancy models and scoring

AI Search uses a relevancy model to compute a relevancy score for each result returned by a search. Documents with higher relevancy scores appear first in the result set. A result’s relevancy score is specific to the particular document, search terms, and user associated with the query.

Each search profile includes its own relevancy model. You cannot view, modify, or delete this relevancy model.

Search signals and machine learning relevancy tuning

AI Search UX components record signals associated with user searches. These search signals include data on how search users interact with the search input field, auto-complete suggestions, facet and navigation tab filters, Genius Result answer cards, and search results.

Machine learning relevancy uses data from these search signals to intelligently tune relevancy models on a continual basis. Every 30 days, AI Search computes a new version of each relevancy model, iteratively modifying its parameters and regression testing it against aggregated search signal data.

When this tuning process is complete, AI Search compares the existing and new relevancy models to see which one produces better matches for user search behavior as recorded in signal data. It selects the better-performing relevancy model, which remains in use until the next tuning cycle begins.

These relevancy model tuning processes occur separately for each search profile. Changes made to the relevancy model in one search profile do not affect relevancy models in other search profiles.

Content security in AI Search

AI Search filters search query results and displays only records that the currently logged in user can access.

Content security is automatically enabled and is not configurable.

Indexed security features

When indexing records from Now Platform tables, AI Search preserves the following access control settings:

- Scripted and non-scripted access control list rules (ACLs)
- User criteria
- Before Query business rules
- Domain separation

Early and late binding security implementations for search queries

At query time, AI Search filters search results by evaluating user access to indexed tables and records. The filtering implementation used depends on the security features present on tables and records that match the search query.
<table>
<thead>
<tr>
<th>Content security implementation</th>
<th>Description</th>
</tr>
</thead>
</table>
| Early binding                   | Default content security implementation that incorporates security filters into the search query. The system adds relevant security filters for the user to each search query. To appear in the search results, records must match the search query and pass all security filters. Early binding security supports non-scripted ACLs, user criteria, Before Query business rules, and domain separation. If a search matches records that have scripted ACLs, the search query automatically falls back to use late binding security.  

**Note:** If an early binding filter produces an error, the search query automatically falls back to use late binding security. |
| Late binding                    | More computationally expensive alternate content security implementation that post-filters search query results. The system applies security filters to the search query just as early binding security does. After retrieving records that match the filtered query, it invokes the GlideRecord.canRead() method for each record. To appear in the search results, records must match the search query, pass all security filters, and return true for the API method. Late binding security supports all indexed security features. By default, late binding security serves as a fallback mechanism for early binding security. Setting the **Force AI Search to use late binding for ACL evaluation** (glide.ais.security.force_late_binding) system property to true forces AI Search to use late binding security for all search queries. |

**Content security for external content**

In the release, does not index security settings for external content. As a result, all users can view all indexed external records as search results.

For more details on using AI Search with external data sources, see Indexing and searching external content in AI Search.

**Encrypted fields in AI Search**

AI Search excludes source record fields encrypted with Encryption Support or Edge Encryption. When dealing with an encrypted source record field, AI Search has the following limitations:

- Content indexing excludes the encrypted field. This exclusion means that search query terms will not match terms from the encrypted field’s content.
- You cannot create a facet using the encrypted field.
• If a search query attempts to filter on the encrypted field, such as when applying an access control list (ACL) filter, the search query fails. An "Encrypted Field is not supported" error message is logged.

For detailed descriptions of the encryption options available for source records, see Encryption.

AI Search logging and debugging

Review AI Search logs and history to analyze performance and diagnose issues. View log messages and ingestion history, or use session debugging to capture detailed messages for a user session.

View AI Search ingestion log messages
Review AI Search ingestion and indexing events by viewing log messages.

Role required: admin

1. Navigate to AI Search > AI Search Logs > Ingestion Warnings & Errors.
   The Log [syslog] table appears with a [Source] [starts with] [AIS-Datasource] filter condition applied.
2. Use the list search, sort, filter, and group functions to locate messages of interest.

View all AI Search log messages
Review AI Search events by viewing log messages.

Role required: admin

1. Navigate to AI Search > AI Search Logs > All.
   The Log [syslog] table appears with a [Message] [contains] [ais] filter condition applied.
2. Use the list search, sort, filter, and group functions to locate messages of interest.

Review ingestion history for an indexed source
View processing results and performance statistics associated with an ingestion event for an indexed source.

Role required: ais_admin

The AI Search Indexed Source History [ais_ingest_datasource_stats] table contains records for indexed source ingestion events. Each record includes performance statistics and processing results for the ingestion event. You can review the ingestion event history record to analyze ingestion performance and diagnose issues.

1. Navigate to AI Search > AI Search Index > Indexed Sources.
2. Edit the indexed source whose indexing history you want to review.
3. In the Indexing History related list, edit the ingestion event record that you want to review.
4. On the Indexed Source History form, review the fields for the selected ingestion event.

**Indexed Source History form fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indexed Source</td>
<td>Reference to the indexed source from which AI Search ingested records for indexing.</td>
</tr>
<tr>
<td>Ingestion Event ID</td>
<td>Sys_id of the ingestion event.</td>
</tr>
<tr>
<td>Partial Ingestion</td>
<td>Option indicating whether AI Search ingested all parent and child tables defined in the indexed source. Valid values:</td>
</tr>
<tr>
<td></td>
<td>• false: AI Search ingested records from the indexed source table and all child tables configured for indexing.</td>
</tr>
<tr>
<td></td>
<td>• true: AI Search only ingested records from a subset of the indexed source tables configured for indexing.</td>
</tr>
</tbody>
</table>
### Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Errors</td>
<td>Count of error messages logged for the ingestion event.</td>
</tr>
<tr>
<td>Number of Minor Errors</td>
<td>Count of minor error messages logged for the ingestion event.</td>
</tr>
<tr>
<td>Number of Warnings</td>
<td>Count of warning messages logged for the ingestion event.</td>
</tr>
<tr>
<td>Ingestion State</td>
<td>State for the ingestion event. Valid values:</td>
</tr>
<tr>
<td></td>
<td>• <strong>cancelled</strong>: Ingestion and indexing did not complete successfully.</td>
</tr>
<tr>
<td></td>
<td>• <strong>indexed</strong>: Ingestion and indexing completed successfully.</td>
</tr>
<tr>
<td></td>
<td>• <strong>indexing</strong>: Ingestion and indexing are ongoing.</td>
</tr>
<tr>
<td></td>
<td>• <strong>not started</strong>: Ingestion and indexing are pending.</td>
</tr>
<tr>
<td>Start Time</td>
<td>System time at which the ingestion event began.</td>
</tr>
<tr>
<td>End Time</td>
<td>System time at which the ingestion event completed.</td>
</tr>
<tr>
<td>Content Preparation Duration</td>
<td>Total time that the Now Platform spent retrieving source records for the ingestion event.</td>
</tr>
<tr>
<td>Indexing Duration</td>
<td>Total time that AI Search spent indexing source records for the ingestion event.</td>
</tr>
<tr>
<td>Records Processed</td>
<td>Count of source records processed for the ingestion event.</td>
</tr>
<tr>
<td>Attachments Processed</td>
<td>Count of source record attachments processed for the ingestion event.</td>
</tr>
<tr>
<td>Documents Processed per Second (DPS)</td>
<td>Average number of source records and attachments processed per second for the ingestion event.</td>
</tr>
</tbody>
</table>

### Enable session debugging for AI Search

Capture and review detailed AI Search log messages for a user session.

Role required: admin

Debugging messages create a log of AI Search events as they occur. Review these messages to diagnose issues or configure optimal performance settings.

When enabled, session debugging is active during the user session or until disabled. For more information on session debugging, see [Session debug](#).

1. To enable debugging, navigate to **System Diagnostics > Session Debug > Debug AI Search**. A message reports completion of the Debug AI Search session debug script.
2. To review debug logs, navigate to **System Diagnostics > Session Debug > Debug Log**. The **Session Log** window opens and displays debug log messages.
3. To disable debugging, navigate to **System Diagnostics > Session Debug > Disable All**. A message reports completion of the Disable All session debug script.
AI Search reference

These reference topics provide additional information about AI Search installed components, system properties, and features.

Plugins installed with AI Search

AI Search adds the following plugin.

AI Search plugins

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>plugin (com.glide.ais)</td>
<td>Enables core functionality for AI Search. Installed in the base system.</td>
</tr>
</tbody>
</table>

Components installed with AI Search

Several types of components are installed with activation of the AI Search plugin, including user roles, scheduled jobs, and tables.

Note: The Application Files table lists the components that are installed with this application. For instructions on how to access this table, see Find components installed with an application.
## Roles installed

<table>
<thead>
<tr>
<th>Role title [name]</th>
<th>Description</th>
<th>Contains roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>administrator [ais_admin]</td>
<td>Manages configuration settings for the application, including the following: • Creates, reads, updates, and deletes indexed sources • Creates, reads, updates, and deletes search sources • Creates and deletes mappings between search sources and search profiles • Creates, reads, updates, and deletes search profiles • Creates, reads, updates, and deletes synonym and stop word dictionaries • Creates and deletes mappings between dictionaries and search profiles • Reads and updates typo handling auto-correction dictionaries linked to search profiles • Creates, reads, updates, and deletes Genius Result configurations • Creates and deletes mappings between Genius Result configurations and search profiles • Creates, reads, updates, and deletes result improvement rules • Creates and deletes mappings between result improvement rules and search profiles This role is included in the Search application administrator [search_application_admin] role.</td>
<td>• None</td>
</tr>
</tbody>
</table>

## Scheduled jobs installed

<table>
<thead>
<tr>
<th>Scheduled job</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregate Health Data for AIS Partition</td>
<td>Collects health check data for AI Search query nodes connected to your instance.</td>
</tr>
<tr>
<td>AI Search Expire Rules</td>
<td>Marks result improvement rules as expired when their end date is in the past.</td>
</tr>
<tr>
<td>AI Search Relevancy Data Processor</td>
<td>Processes search signal data as part of search profile relevancy model tuning by the machine learning relevancy feature.</td>
</tr>
<tr>
<td>Scheduled job</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>AIS Collect Ingestion Stats</td>
<td>Collects ingestion history statistics for indexed sources.</td>
</tr>
<tr>
<td>AIS Derived Dictionary Auto Refresh</td>
<td>Refreshes derived typo handling dictionaries when their refresh interval has elapsed.</td>
</tr>
<tr>
<td>AIS Index Event Processor</td>
<td>Processes indexing events for indexed sources.</td>
</tr>
<tr>
<td>AIS Index Event Queue Size Monitor</td>
<td>Monitors the size of the indexing queue during indexing of source records.</td>
</tr>
<tr>
<td>AIS Validate Publish ID and Auto Publish</td>
<td>Publishes search profiles and typo handling, stop word, and synonym dictionaries.</td>
</tr>
<tr>
<td>ML Trigger for AIS Search Relevancy</td>
<td>Triggers automatic tuning of search profile relevancy models by the machine learning relevancy feature.</td>
</tr>
</tbody>
</table>

### Tables installed

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI Search ACL Overrides [ais_acl_overrides]</td>
<td>List of rules used by content security.</td>
</tr>
<tr>
<td>AI Search Child Table [ais_child_table]</td>
<td>List of child tables defined for indexed sources.</td>
</tr>
<tr>
<td>AI Search Configuration Attribute [ais_configuration_attribute]</td>
<td>List of indexed source attributes available for use in indexed sources.</td>
</tr>
<tr>
<td>AI Search Connection [ais_connection]</td>
<td>List of AI Search query nodes connected to your instance.</td>
</tr>
<tr>
<td>AI Search Dictionary [ais_dictionary]</td>
<td>List of typo handling, stop word, and synonym dictionaries.</td>
</tr>
<tr>
<td>AI Search Dictionary Term [ais_dictionary_term]</td>
<td>List of terms defined in typo handling, stop word, and synonym dictionaries.</td>
</tr>
<tr>
<td>AI Search Genius Result Configuration NLU Model Mapping [ais_genius_result_configuration_sys_nlu_model_m2m]</td>
<td>List of mappings between NLU models and Genius Result configurations.</td>
</tr>
<tr>
<td>AI Search Genius Result Configuration [ais_genius_result_configuration]</td>
<td>List of Genius Result configurations.</td>
</tr>
<tr>
<td>AI Search Index Events stats [ais_index_queue_stats]</td>
<td>List of statistics entries for indexing events.</td>
</tr>
<tr>
<td>AI Search Indexed Retry History [ais_ingest_retry_stats]</td>
<td>List of ingestion history events produced when retrying indexing for a source table record.</td>
</tr>
<tr>
<td>AI Search Indexed Source [ais_datasource]</td>
<td>List of indexed sources.</td>
</tr>
<tr>
<td>AI Search Indexed Source Attribute [ais_datasource_attribute]</td>
<td>List of indexed source attributes configured for indexed sources.</td>
</tr>
<tr>
<td>AI Search Indexed Source Field Attribute [ais_datasource_field_attribute]</td>
<td>List of field settings configured for indexed sources.</td>
</tr>
<tr>
<td>AI Search Indexed Source History [ais_ingest_datasource_stats]</td>
<td>List of ingestion history events for indexed sources.</td>
</tr>
<tr>
<td>AI Search Indexed Table History [ais_ingest_table_stats]</td>
<td>List of ingestion history events for individual source tables defined in indexed sources.</td>
</tr>
<tr>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>AI Search Partition Health [ais_partition_health]</td>
<td>List of health check events for AI Search query nodes connected to your instance.</td>
</tr>
<tr>
<td>AI Search Partition Health Response [ais_partition_health_response]</td>
<td>List of health check response events for AI Search query nodes connected to your instance.</td>
</tr>
<tr>
<td>AI Search Publish History [ais_publish_history]</td>
<td>List of publication history events for search profiles and typo handling, stop word, and synonym dictionaries.</td>
</tr>
<tr>
<td>AI Search Relevancy Auto Train Solution [ais_relevancy_autotrain_solution]</td>
<td>List of relevancy model tuning records used by machine learning relevancy.</td>
</tr>
<tr>
<td>AI Search Relevancy Solution Definition [ais_relevancy_solution_definition]</td>
<td>List of search profiles with relevancy models tuned by machine learning relevancy.</td>
</tr>
<tr>
<td>AI Search Relevancy Training Execution [ais_relevancy_training_execution]</td>
<td>List of relevancy model tuning tasks performed by machine learning relevancy.</td>
</tr>
<tr>
<td>AI Search Relevancy Training Staging [ais_relevancy_training_staging]</td>
<td>List of relevancy model staging tasks performed by machine learning relevancy.</td>
</tr>
<tr>
<td>AI Search Results Improvement Rule [ais_rule]</td>
<td>List of result improvement rules.</td>
</tr>
<tr>
<td>AI Search Results Improvement Rule Action [ais_rule_action]</td>
<td>List of actions defined for use in result improvement rules.</td>
</tr>
<tr>
<td>AI Search Results Improvement Rule Condition Builder Values [v_ais_result_improvement_rule_condition_builder_values]</td>
<td>List of static values defined for use in result improvement rule actions.</td>
</tr>
<tr>
<td>AI Search Search Profile [ais_search_profile]</td>
<td>List of search profiles.</td>
</tr>
<tr>
<td>AI Search Search Profile Dictionary Mapping [ais_search_profile_ais_dictionary_m2m]</td>
<td>List of mappings between search profiles and typo handling, stop word, and synonym dictionaries.</td>
</tr>
<tr>
<td>AI Search Search Profile Genius Result Configuration Mapping [ais_search_profile_ais_genius_result_configuration_m2m]</td>
<td>List of mappings between search profiles and Genius Result configurations.</td>
</tr>
<tr>
<td>AI Search Search Profile Relevancy Model [ais_search_profile_relevancy_model]</td>
<td>List of relevancy models created by machine learning relevancy.</td>
</tr>
<tr>
<td>AI Search Search Profile Search Source Mapping [ais_search_profile_ais_search_source_m2m]</td>
<td>List of mappings between search profiles and search sources.</td>
</tr>
<tr>
<td>AI Search Search Source [ais_search_source]</td>
<td>List of search sources.</td>
</tr>
</tbody>
</table>
**AI Search system properties**

Users with the admin role can configure the following system properties for AI Search by navigating to System Properties > AI Search.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.ais.genius_result.enabled</td>
<td>Option to enable Genius Results in search queries.</td>
</tr>
<tr>
<td></td>
<td>- Type: Boolean</td>
</tr>
<tr>
<td></td>
<td>- Default value: <strong>false</strong></td>
</tr>
<tr>
<td></td>
<td>- Supported values:</td>
</tr>
<tr>
<td></td>
<td>• <strong>true</strong>: Genius Results are enabled in search queries. Results for a given search may be inconsistent from query to query.</td>
</tr>
<tr>
<td></td>
<td>• <strong>false</strong>: Genius Results are disabled in search queries. Search query results should be consistent.</td>
</tr>
<tr>
<td></td>
<td>- Location: System Properties [sys_properties] table</td>
</tr>
<tr>
<td>glide.ais.ha.auto_switch_to_near_node</td>
<td>Option to enable automatic switch over to a healthy AI Search node in the near datacenter.</td>
</tr>
<tr>
<td></td>
<td>- Type: Boolean</td>
</tr>
<tr>
<td></td>
<td>- Default value: <strong>true</strong></td>
</tr>
<tr>
<td></td>
<td>- Supported values:</td>
</tr>
<tr>
<td></td>
<td>• <strong>true</strong>: The system automatically switches over to use an AI Search node in the near datacenter when its read health score equals or exceeds the glide.ais.monitor.health_threshold_green threshold.</td>
</tr>
<tr>
<td></td>
<td>• <strong>false</strong>: The system does not automatically switch over to an AI Search node in the near datacenter.</td>
</tr>
<tr>
<td></td>
<td>- Location: System Properties [sys_properties] table</td>
</tr>
<tr>
<td>glide.ais.ha.enable_auto_failover</td>
<td>Option to enable automatic failover to an alternate AI Search node when the active node becomes unhealthy.</td>
</tr>
<tr>
<td></td>
<td>- Type: Boolean</td>
</tr>
<tr>
<td></td>
<td>- Default value: <strong>true</strong></td>
</tr>
<tr>
<td></td>
<td>- Supported values:</td>
</tr>
<tr>
<td></td>
<td>• <strong>true</strong>: The system automatically fails over to an alternate AI Search node if the active node’s write health score drops below the glide.ais.monitor.health_threshold_yellow threshold.</td>
</tr>
<tr>
<td></td>
<td>• <strong>false</strong>: The system does not automatically fail over an active partition based on its health score.</td>
</tr>
<tr>
<td></td>
<td>- Location: System Properties [sys_properties] table</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>glide.ais.ingestion.batcher_queue_memory_size</td>
<td>Size in MB of batcher queue for indexing of source record content.</td>
</tr>
<tr>
<td></td>
<td>• Type: Integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 20</td>
</tr>
<tr>
<td></td>
<td>• Location: System Properties [sys_properties] table</td>
</tr>
<tr>
<td>glide.ais.ingestion.batcher_queue_size</td>
<td>Maximum number of records on batcher queue for indexing of source record content.</td>
</tr>
<tr>
<td></td>
<td>• Type: Integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 1,000</td>
</tr>
<tr>
<td></td>
<td>• Location: System Properties [sys_properties] table</td>
</tr>
<tr>
<td>glide.ais.ingestion.dictionary_term_batcher_queue_size</td>
<td>Maximum count of records on queue for addition of terms to a synonym, stop word, or typo handling dictionary.</td>
</tr>
<tr>
<td></td>
<td>• Type: Integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 1,000</td>
</tr>
<tr>
<td></td>
<td>• Location: System Properties [sys_properties] table</td>
</tr>
<tr>
<td>glide.ais.ingestion.failure_retry_timeout</td>
<td>Timeout period in seconds for indexing of content from a source record.</td>
</tr>
<tr>
<td></td>
<td>• Type: Integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 600</td>
</tr>
<tr>
<td></td>
<td>• Location: System Properties [sys_properties] table</td>
</tr>
<tr>
<td>glide.ais.ingestion.feedback_logger_error</td>
<td>Destination for AI Search ingestion feedback messages with the ERROR level.</td>
</tr>
<tr>
<td></td>
<td>• Type: String</td>
</tr>
<tr>
<td></td>
<td>• Default value: <strong>Sys Log</strong></td>
</tr>
<tr>
<td></td>
<td>• Supported values:</td>
</tr>
<tr>
<td></td>
<td>• <strong>None</strong>: Do not log ingestion feedback messages with this level.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Sys Log</strong>: Log ingestion feedback messages with this level to the system log.</td>
</tr>
<tr>
<td></td>
<td>• <strong>File Log</strong>: Log ingestion feedback messages with this level to a log file on the active node.</td>
</tr>
<tr>
<td></td>
<td>• Location: System Properties [sys_properties] table</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| glide.ais.ingestion.feedback_logger_info | Destination for AI Search ingestion feedback messages with the INFO level.  
  - Type: String  
  - Default value: **None**  
  - Supported values:  
    - **None**: Do not log ingestion feedback messages with this level.  
    - **Sys Log**: Log ingestion feedback messages with this level to the system log.  
    - **File Log**: Log ingestion feedback messages with this level to a log file on the active node.  
  - Location: System Properties [sys_properties] table |
| glide.ais.ingestion.feedback_logger_minor_error | Destination for AI Search ingestion feedback messages with the MINOR_ERROR level.  
  - Type: String  
  - Default value: **Sys Log**  
  - Supported values:  
    - **None**: Do not log ingestion feedback messages with this level.  
    - **Sys Log**: Log ingestion feedback messages with this level to the system log.  
    - **File Log**: Log ingestion feedback messages with this level to a log file on the active node.  
  - Location: System Properties [sys_properties] table |
| glide.ais.ingestion.feedback_logger_warn | Destination for AI Search ingestion feedback messages with the WARN level.  
  - Type: String  
  - Default value: **Sys Log**  
  - Supported values:  
    - **None**: Do not log ingestion feedback messages with this level.  
    - **Sys Log**: Log ingestion feedback messages with this level to the system log.  
    - **File Log**: Log ingestion feedback messages with this level to a log file on the active node.  
  - Location: System Properties [sys_properties] table |
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| glide.ais.monitor.health_status_check_interval | Interval in seconds between AI Search partition health status checks.  
  - Type: Integer  
  - Default value: 60  
  - Location: System Properties [sys_properties] table |
| glide.ais.monitor.health_status_check_timeout | Timeout period in seconds for AI Search partition health status checks.  
  - Type: Integer  
  - Default value: 30  
  - Location: System Properties [sys_properties] table |
| glide.ais.monitor.health_threshold_green | Inclusive lower percentage bound for green partition health score range. The inclusive upper bound for this health score range is 100.  
  - Type: Integer  
  - Default value: 90  
  - Location: System Properties [sys_properties] table |
| glide.ais.monitor.health_threshold_yellow | Inclusive lower percentage bound for yellow partition health score range. The non-inclusive upper bound for this health score range is set by the glide.ais.monitor.health_threshold_green property value.  
  The red partition health score range includes all scores below this property value. If the health score for an active partition drops into the red range, and if glide.ais.ha.enable_auto_failover is set to true, AI Search failover on the partition.  
  - Type: Integer  
  - Default value: 50  
  - Location: System Properties [sys_properties] table |
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.ais.security.force_late_binding</td>
<td>Option to force use of the late binding security implementation for all search queries. For descriptions of the early binding and late binding security implementations, see Content security in AI Search.</td>
</tr>
<tr>
<td></td>
<td>• Type: Boolean</td>
</tr>
<tr>
<td></td>
<td>• Default value: false</td>
</tr>
<tr>
<td></td>
<td>• Supported values:</td>
</tr>
<tr>
<td></td>
<td>• true: The system uses the late binding security implementation for all search queries.</td>
</tr>
<tr>
<td></td>
<td>• false: The system uses the early binding security implementation for search queries. If search results include scripted ACLs, or if early binding encounters an error, the system switches to use the late binding security implementation.</td>
</tr>
<tr>
<td></td>
<td>• Location: System Properties [sys_properties] table</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You can enable the late binding security implementation for all search results from a particular indexed source by setting the Force Late Binding field to true for the indexed source.</td>
</tr>
<tr>
<td>glide.ais.query.max_request_count_per_search</td>
<td>Maximum number of requests that an AI Search node can process per search query.</td>
</tr>
<tr>
<td></td>
<td>• Type: Integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 10</td>
</tr>
<tr>
<td></td>
<td>• Location: System Properties [sys_properties] table</td>
</tr>
<tr>
<td>glide.ais.query.requested_rows_multiplier</td>
<td>Result-count multiplier for search queries that use the late binding security implementation. The system multiplies the search query's minimum desired result count by this factor before requesting records from the AI Search node. Extra records replace any search results removed by the late binding security implementation. For example, with the default value of 3, a search query that uses the late binding security implementation and expects at least 10 results produces a request to the AI Search node for 30 matching records. The final result set includes the first 10 of these records that the user can access. Lower values improve search query performance but may reduce search result count below the requested minimum.</td>
</tr>
<tr>
<td></td>
<td>• Type: Integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 3</td>
</tr>
<tr>
<td></td>
<td>• Location: System Properties [sys_properties] table</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>glide.ais.query.search_operator</td>
<td>Boolean search operator to use when a search query includes multiple terms. When using the AND (conjunctive) operator, search only finds records that include all search query terms and phrases. When using the OR (disjunctive) operator, search finds records that include any search query term or phrase.</td>
</tr>
<tr>
<td>Type: String</td>
<td>Default value: <strong>AND_OR</strong></td>
</tr>
<tr>
<td>Supported values:</td>
<td></td>
</tr>
<tr>
<td>• <strong>AND then OR query</strong>: Search using the AND operator. If the search query returns less than one full page of results, automatically resubmit it using the OR operator. The resubmitted search query only finds records that contain at least half (rounded up) of the terms and phrases in the OR expression.</td>
<td></td>
</tr>
<tr>
<td>• <strong>OR query</strong>: Search using the OR operator.</td>
<td></td>
</tr>
<tr>
<td>• Location: System Properties [sys_properties] table</td>
<td></td>
</tr>
<tr>
<td>glide.mlpredictor.ml_x_snc_global_global_6eedb38234bf5010f877396127c8ffee.predict.request_timeout</td>
<td>Timeout period for ML predictions used in Genius Result processing. If Genius Result processing time exceeds this value for a search query, no Genius Result answers are displayed in the search query results.</td>
</tr>
<tr>
<td>Type: Integer</td>
<td>Default value: <strong>1000</strong></td>
</tr>
<tr>
<td>Location: System Properties [sys_properties] table</td>
<td></td>
</tr>
</tbody>
</table>

**Now Platform tables excluded from AI Search indexing**

AI Search excludes the following Now Platform tables when indexing content. You cannot configure these tables, or tables derived from them, as AI Search indexed sources.

- Base Configuration Item [cmdb]
- Email [sys_email]
- Event [sysevent]
- Import Set Row [sys_import_set_row]
- Log [syslog]
- Queue [ecc_queue]
- Replicated Operation [sys_replication_queue]
- Sys Audit [sys_audit]
- Task [task]

**AI Search index fields**

List of fields available on records in the AI Search index. Data from fields on source records maps to these fields during indexing.
## AI Search index fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ai_search_parent_title</td>
<td>This field is automatically generated by AI Search.</td>
</tr>
<tr>
<td>ai_search_teaser_text</td>
<td>This field is automatically generated by AI Search.</td>
</tr>
<tr>
<td>ai_search_teaser_title</td>
<td>This field is automatically generated by AI Search.</td>
</tr>
<tr>
<td>datasource_id</td>
<td>Name of the indexed data source that added the record to the AI Search index.</td>
</tr>
<tr>
<td>ext_record_id</td>
<td>Unique identifier for the external data source record that corresponds to the indexed record. Only populated for records from external data sources.</td>
</tr>
<tr>
<td>index_event_id</td>
<td>Sys_id of the indexing event that added the record to the AI Search index.</td>
</tr>
<tr>
<td>language</td>
<td>Language configured for the source record in its Now Platform table.</td>
</tr>
<tr>
<td>record_class_name</td>
<td>The hierarchical class used to render the source record.</td>
</tr>
<tr>
<td>sys_id</td>
<td>Sys_id for the source record.</td>
</tr>
<tr>
<td>table</td>
<td>For records from Now Platform tables, this index field indicates the name of the source table. For records from external data sources, this index field indicates the name of the content schema table specified during document ingestion.</td>
</tr>
<tr>
<td>text</td>
<td>Searchable text for the indexed record. Displayed in search results.</td>
</tr>
<tr>
<td>title</td>
<td>Title for the indexed record. Displayed in search results.</td>
</tr>
</tbody>
</table>

### Common index fields

The following AI Search index fields appear on all records indexed from Now Platform source tables:

- ai_search_parent_title
- ai_search_teaser_text
- ai_search_teaser_title
- record_class_name
- sys_id
- table
Extending AI Search with ServiceNow Store applications

Install applications from the ServiceNow® Store to extend AI Search functionality and gain insight into search usage and behavior.

Analytics and Reporting Solution for Advanced Management Tools

ServiceNow® Analytics and Reporting Solutions contain prepackaged Performance Analytics and Reporting content for use with other Now Platform products. This Analytics and Reporting Solution helps AI Search administrators analyze search query traffic trends, review indexed record and configuration settings, and preview search query results.

Required roles

The following roles are associated with this solution:

- Now Platform administrator (admin): Install and activate this Analytics and Reporting Solution and make any necessary changes to system properties.
- AI Search administrator (ais_admin): Review the AI Search dashboards. Share the dashboards with appropriate stakeholders. Test search queries using the Search Preview UI module.
- User Experience Analytics administrator (analytics_admin), User Experience Analytics viewer (analytics_viewer), User Portal Analytics administrator (portal_analytics_admin), Portal Analytics viewer(portal_analytics_viewer), Web Analytics administrator (web_analytics_admin), or Web Analytics viewer(web_analytics_viewer): View the Search Analytics dashboard metrics and reports.
- Impersonator (impersonator): View NLU intents detected in queries, enable debugging, or search as another user in the Search Preview UI module.

Activate the Analytics and Reporting Solution for Advanced Management Tools

Activate the content pack ServiceNow® Store application for the Analytics and Reporting Solution.

The User Experience Analytics API application from the ServiceNow Store must be activated in your instance.

Role required: admin

1. Navigate to System Applications > All Available Applications > Available To Obtain From Store.
2. Browse for Advanced Management Tools and verify that you have the necessary valid entitlements.
   You need a Now Support account and permission to request applications for the instances under consideration. The Now Support account and the instance must be part of the same company. For more information, see Install a ServiceNow Product on the ServiceNow Store.
4. Install the application.

The following application menus and modules appear in the application navigator:

<table>
<thead>
<tr>
<th>Application</th>
<th>Application navigator path</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI Search Profile dashboard</td>
<td>AI Search &gt; AI Search Analytics &gt; Search Profile Analytics</td>
</tr>
<tr>
<td>AI Search dashboard</td>
<td>AI Search &gt; AI Search Analytics &gt; Search Index Analytics</td>
</tr>
<tr>
<td>Search preview UI</td>
<td>AI Search &gt; Preview &gt; Search Preview</td>
</tr>
</tbody>
</table>
Populate data tables for the Search Analytics dashboard

Execute the scheduled job that populates data tables used by metrics, trends, and reports on the Search Analytics dashboard.

Role required: admin

The Advanced Management Tools application includes a `AISearchAnalyticsGlobalScheduledJobUtils` scheduled job. Execute this scheduled job to begin populating tables needed for data visualizations on the Search Analytics dashboard. Until the first job run completes, some elements on the Search Analytics dashboard display no data.

1. In the navigation filter, enter `sys_trigger.list`.
2. Edit the `AISearchAnalyticsGlobalScheduledJobUtils` scheduled job.
3. Click Execute Now.

The `AISearchAnalyticsGlobalScheduledJobUtils` scheduled job populates the data tables needed by the Search Analytics dashboard. To keep the tables current, the system runs this scheduled job again every day around midnight. You do not need to run this job again.

Note: The exact run time for the scheduled job may vary by a few hours depending on server resource availability.

If you uninstall the Advanced Management Tools application, disable the scheduled job by following the steps in Disable population of data tables for the Search Analytics dashboard.

Disable population of data tables for the Search Analytics dashboard

Delete the scheduled job that populates data tables used by metrics, trends, and reports on the Search Analytics dashboard.

Only perform this task if you uninstall the Advanced Management Tools application after enabling the `AISearchAnalyticsGlobalScheduledJobUtils` scheduled job. For the steps to enable this scheduled job, see Populate data tables for the Search Analytics dashboard.

Role required: admin

After uninstalling the Advanced Management Tools application, delete the scheduled job that populates the Search Analytics dashboard with search user data.

1. In the navigation filter, enter `sys_trigger.list`.
2. Edit the `AISearchAnalyticsGlobalScheduledJobUtils` scheduled job.
3. Click Delete.

The `AISearchAnalyticsGlobalScheduledJobUtils` scheduled job no longer runs and populates the data tables needed for the Search Analytics dashboard.
**AI Search Profile dashboard**

The AI Search Profile dashboard summarizes indexed record counts and search query traffic associated with a search profile defined in AI Search. Interactive filters enable users to choose a search profile and select the time frame for analysis of search query traffic.
To access the dashboard, navigate to **AI Search > AI Search Analytics > Search Profile Analytics.**

**Note:** If the dashboard displays a Read operation on table '<name>' from scope 'Advanced AI Search Management Tools' was denied informational message, ask your administrator to perform the steps described in Create a cross-scope access privilege for the AI Search dashboards for the listed table.

**Required Now Platform roles**

- The ais_admin role is required to view or edit the dashboard

**Use cases**

For examples of how different people in your organization would use this dashboard, see these use cases.

<table>
<thead>
<tr>
<th>User</th>
<th>Dashboard use</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI Search administrator</td>
<td>Reviews indexed record counts and follows search query traffic trends for search profiles defined in AI Search.</td>
</tr>
</tbody>
</table>

**Reports**

<table>
<thead>
<tr>
<th>Title</th>
<th>Type</th>
<th>Source table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Searchable Documents</td>
<td>Single Score</td>
<td>sn_ais_admin_tools_ai_search_dashboard_documents_by_search_profile</td>
<td>Shows the number of indexed records that users can find when searching with the selected search profile.</td>
</tr>
<tr>
<td>Documents by Search Source</td>
<td>Donut</td>
<td>sn_ais_admin_tools_ai_search_dashboard_documents_by_search_source</td>
<td>Shows the number of indexed records accessible from each search source linked to the selected search profile.</td>
</tr>
<tr>
<td>Queries by Application</td>
<td>Bar</td>
<td>sys_search_event</td>
<td>Shows the number of search queries that used the selected search profile in the selected query time frame, grouped by search application.</td>
</tr>
<tr>
<td>Title</td>
<td>Type</td>
<td>Source table</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------</td>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Queries Run Against This Profile</td>
<td>Line</td>
<td>sys_search_event</td>
<td>Shows the number of search queries that used the selected search profile in the selected query time frame, grouped by month.</td>
</tr>
</tbody>
</table>
**AI Search dashboard**

The AI Search dashboard summarizes AI Search indexed documents, configuration settings in use, and search query traffic. An interactive filter enables users to select the time frame for analysis of search query traffic.
Al Search dashboard - AI Search Query tab
To access the dashboard, navigate to **AI Search > AI Search Analytics > Search Index Analytics**.

**Note:** If the dashboard displays a Read operation on table '<name>' from scope 'Advanced AI Search Management Tools' was denied informational message, ask your administrator to perform the steps described in Create a cross-scope access privilege for the AI Search dashboards for the listed table.

**Required Now Platform roles**

- ais_admin, required to view or edit the dashboard

**Use cases**

For examples of how different people in your organization would use this dashboard, see these use cases.

<table>
<thead>
<tr>
<th>User</th>
<th>Dashboard use</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI Search administrator</td>
<td>Reviews indexed record counts and follows search query traffic trends for AI Search.</td>
</tr>
</tbody>
</table>

**Reports**

**AI Search Index tab**

<table>
<thead>
<tr>
<th>Title</th>
<th>Type</th>
<th>Source table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indexed Documents</td>
<td>Single Score</td>
<td>sn_ais_admin_tools_ai_search_dashboard_tool_indexed_documents</td>
<td>Shows the number of searchable records indexed by AI Search.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>To drill down and view searchable records for an indexed source grouped by source table, click the graph segment for that indexed source. Refresh the report to return to the top-level view.</td>
</tr>
<tr>
<td>Documents by Indexed Source</td>
<td>Donut</td>
<td>sn_ais_admin_tools_ai_search_dashboard_tool_indexed_documents</td>
<td>Shows the number of searchable records indexed by AI Search, grouped by indexed source.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>To drill down and view searchable records for an indexed source grouped by source table, click the graph segment for that indexed source. Refresh the report to return to the top-level view.</td>
</tr>
<tr>
<td>Title</td>
<td>Type</td>
<td>Source table</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------</td>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Search Profiles</td>
<td>Single Score</td>
<td>ais_search_profile</td>
<td>Shows the number of search profiles defined in AI Search.</td>
</tr>
<tr>
<td>Indexed Sources</td>
<td>Single Score</td>
<td>ais_datasource</td>
<td>Shows the number of indexed sources defined in the AI Search index.</td>
</tr>
<tr>
<td>Search Applications</td>
<td>Single Score</td>
<td>sys_search_context_config</td>
<td>Shows the number of search application configurations defined that use the AI Search search engine.</td>
</tr>
<tr>
<td>Dictionaries</td>
<td>Single Score</td>
<td>ais_dictionary</td>
<td>Shows the number of synonym and stop word dictionaries defined in AI Search.</td>
</tr>
<tr>
<td>Configured Genius Results</td>
<td>Single Score</td>
<td>ais_genius_result_configuration</td>
<td>Shows the number of Genius Result configurations defined in AI Search.</td>
</tr>
<tr>
<td>Title</td>
<td>Type</td>
<td>Source table</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>---------------</td>
<td>--------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Results Improvement Rules</td>
<td>Single Score</td>
<td>ais_rule</td>
<td>Shows the number of result improvement rules defined in AI Search.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[42]</td>
<td></td>
</tr>
<tr>
<td>Documents by Search Profile</td>
<td>Bar</td>
<td>sn_ais_admin_tools_ai_search_dashboard_documents_by_search_profile</td>
<td>Shows the number of indexed records searchable through each search profile defined in AI Search.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[ ]</td>
<td></td>
</tr>
<tr>
<td>New Documents Indexed by Month</td>
<td>Bar</td>
<td>sn_ais_admin_tools_ai_search_dashboard_documents_by_month</td>
<td>Shows the number of indexed records grouped by month.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[ ]</td>
<td></td>
</tr>
</tbody>
</table>

**AI Search Query tab**

<table>
<thead>
<tr>
<th>Title</th>
<th>Type</th>
<th>Source table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queries by Search Profile</td>
<td>Donut</td>
<td>sys_search_event</td>
<td>Shows the number of search queries in the selected time frame, grouped by search profile used.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[ ]</td>
<td></td>
</tr>
<tr>
<td>Queries by Language</td>
<td>Donut</td>
<td>sys_search_event</td>
<td>Shows the number of search queries in the selected time frame, grouped by query language (Now Platform language context).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[ ]</td>
<td></td>
</tr>
<tr>
<td>Queries Run Against Index</td>
<td>Line</td>
<td>sys_search_event</td>
<td>Shows the number of search queries in the selected time frame, grouped by month.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[ ]</td>
<td></td>
</tr>
</tbody>
</table>
Create a cross-scope access privilege for the AI Search dashboards
Enable the AI Search dashboards to read records from tables that cannot be accessed from the Advanced Management Tools application scope.

Role required: admin

The AI Search Profile and AI Search dashboards belong to the Advanced Management Tools application scope. If an indexed source or search source table cannot be accessed from this scope, the dashboards display the following informational message:

Read operation on table '<name>' from scope 'Advanced AI Search Management Tools' was denied. The application 'Advanced AI Search Management Tools' must declare a cross scope access privilege. Please contact the application author to update their privilege requests.

To resolve this issue, define a cross-scope table access privilege for the Advanced Management Tools application.

For more information on cross-scope privileges, see Cross-scope privilege record.

1. Set your current application scope context to Advanced Management Tools using the application picker.
3. Click New.
4. On the Cross scope privilege form, enter the following field values.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Scope</td>
<td>&lt;table scope&gt;</td>
</tr>
<tr>
<td>Target Name</td>
<td>&lt;table name&gt;</td>
</tr>
<tr>
<td>Target Type</td>
<td>Table</td>
</tr>
<tr>
<td>Operation</td>
<td>Read</td>
</tr>
<tr>
<td>Status</td>
<td>Allowed</td>
</tr>
</tbody>
</table>

5. Click Submit.

The new cross-scope privilege appears in the Cross scope privilege table.
Search Analytics dashboard
The Search Analytics dashboard displays key performance metrics, trends, and reports for AI Search usage. Interactive filters enable analysts to view performance analytics for individual search applications and to select the time frame to analyze.
To access the Search Analytics dashboard, navigate to **User Experience Analytics > Dashboard** and click the AI Search Analytics icon ( ) or link in the modules menu. To learn more about the User Experience Analytics dashboard, see **Overview of the dashboard**.

### Required Now Platform roles

To view the Search Analytics dashboard, you must have one of the following roles:

- analytics_admin
- analytics_viewer
- portal_analytics_admin
- portal_analytics_viewer
- web_analytics_admin
- web_analytics_viewer

### Use cases

For examples of how different people in your organization would use this dashboard, see these use cases.

<table>
<thead>
<tr>
<th>User</th>
<th>Dashboard use</th>
</tr>
</thead>
</table>
| Any of the following:  
  - Portal Analytics administrator or viewer  
  - User Experience Analytics administrator or viewer  
  - Web Analytics administrator or viewer |  
  - View and monitor search usage and search performance for a specified search application and date range  
  - Review search trends to better understand the needs of search application end users  
  - Gain insights on how to improve search experience and knowledge coverage |

### Interactive filters

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search application</td>
<td>Specifies the search application to use when populating search analytics metrics, trends, and reports. You can search for an application or click its name in the list. Click <strong>Apply</strong> to make your filter selection take effect.</td>
</tr>
<tr>
<td>Date range</td>
<td>Specifies the range of dates to use when populating search analytics metrics, trends, and reports. By default, the dashboard displays data from the last 30 days. You can choose one of the preset date ranges or set your own start and end dates. Click <strong>Apply</strong> to make your filter selection take effect.</td>
</tr>
</tbody>
</table>

*Note:* You can only select a single search application at a time.
## Metrics, trends, and reports

<table>
<thead>
<tr>
<th>Title</th>
<th>Report type</th>
<th>Source tables</th>
<th>Description</th>
</tr>
</thead>
</table>
| Search users           | Line        | • Metric and trend: AI Search Analytics Dashboard Unique Search Users [sn AIS Admin Tools Ai Search Analytics Dashboard Unique Search Users](sn_ais_admin_tools_ai_search_analytics_dashboard_unique_search_users)  
• Report: AI Search Analytics Dashboard Daily Search Users [sn ais admin tools ai_search_analytics_dashboard_daily_search_users](sn_ais_admin_tools_ai_search_analytics_dashboard_daily_search_users) | • Metric indicates the total count of unique users who submitted search queries in the selected date range.  
• Trend describes how the number of unique search users changed in the selected date range.  
• Report displays the number of unique search users for dates in the selected range.  

**Note:** Searches performed while impersonating another user are ignored for this metric, trend, and report. |
| Total searches         | Line        | AI Search Analytics Dashboard Total Searches by Date [sn ais admin tools ai_search_analytics_dashboard_total_searches_by_date](sn_ais_admin_tools_ai_search_analytics_dashboard_total_searches_by_date) | • Metric indicates the total count of search queries submitted in the selected date range.  
• Trend describes how the count of search queries submitted changed in the selected date range.  
• Report displays the count of search queries submitted for dates in the selected range. |
<table>
<thead>
<tr>
<th>Title</th>
<th>Report type</th>
<th>Source tables</th>
<th>Description</th>
</tr>
</thead>
</table>
| Average response time | Line        | • Metric and trend: AI Search Analytics Dashboard Average Search Response Time [sn_ais_admin_tools_ai_search_analytics_dashboard_average_response_time]  
 • Report: AI Search Analytics Dashboard Daily Average Response Time [sn_ais_admin_tools_ai_search_analytics_dashboard_daily_average_response_time]  
 • Metric indicates the average search query response time for the selected date range.  
 • Trend describes how the average search query response time changed in the selected date range.  
 • Report displays the average search query response time for dates in the selected range. |
| Average click position| Line        | • Metric and trend: AI Search Analytics Dashboard Average Click Position [sn_ais_admin_tools_ai_search_analytics_dashboard_average_click_position]  
 • Report: AI Search Analytics Dashboard Daily Average Click Position [sn_ais_admin_tools_ai_search_analytics_dashboard_daily_average_click_position]  
 • Metric indicates the average position of user-selected search query results for the selected date range.  
 • Trend describes how the average position of user-selected search query results changed in the selected date range.  
 • Report displays the average position of user-selected search query results for dates in the selected range. |
| Searches over time    | Line        | AI Search Analytics Dashboard Total Searches by Date [sn_ais_admin_tools_ai_search_analytics_dashboard_total_searches_by_date]  
 • The count of search queries submitted for dates in the selected range. |

Note: Positions indicate result numbers. For example, a position of 2 means that the user selected the second result returned for a search query.
<table>
<thead>
<tr>
<th>Title</th>
<th>Report type</th>
<th>Source tables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top clicked results</td>
<td>Horizontal Bar</td>
<td>AI Search Analytics Dashboard Trending Search Content</td>
<td>The most frequently clicked search results in the selected date range.</td>
</tr>
<tr>
<td>Top searches</td>
<td>Horizontal Bar</td>
<td>AI Search Analytics Dashboard Trending Search Terms</td>
<td>The most frequently submitted search queries in the selected date range.</td>
</tr>
<tr>
<td>Genius Results (triggered vs. clicked)</td>
<td>Horizontal Bar</td>
<td>AI Search Analytics Dashboard Trending Genius Result</td>
<td>The search queries that produced the highest proportion of triggered and selected Genius Result configurations in the selected date range.</td>
</tr>
<tr>
<td>Searches with no clicks</td>
<td>Horizontal Bar</td>
<td>sn_ais_admin_tools_search_event_interaction_analytics</td>
<td>The most frequently submitted search queries in the selected date range for which users did not select any search result.</td>
</tr>
<tr>
<td>Searches with no results</td>
<td>Horizontal Bar</td>
<td>sn_ais_admin_tools_search_event_interaction_analytics</td>
<td>The most frequently submitted search queries in the selected date range that produced no results.</td>
</tr>
</tbody>
</table>

**Search Preview UI for AI Search**

The Search Preview UI enables you to test AI Search queries using settings from a selected search profile. Administrator tools help you review search query performance data and feedback, debug queries, and override default query settings for testing purposes.

Access the Search Preview UI by navigating to **AI Search > Preview > Search Preview.**
Required Now Platform roles

- The ais_admin role is required to view and use the Search Preview UI
- The impersonator role is required for some AI Search administrator tools
Search Preview UI components

1. Service Portal Option, Search Profile
2. Delete email
3. Table
4. Genius Results for delete email
5. Showing results 1 - 10 for delete email
6. Process Data

Query Rules Triggered: 0
Intents Matched: 1
catalogFind
Total time: 3051ms
Pre-processing time: 34ms
Search query time: 205ms
GeniusResult computation: 2792ms
Security processing time: 56ms
## Search Preview UI components

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Search profile list</td>
<td>Select the search profile to apply when previewing search queries.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The list only includes published search profiles that have one or more linked search sources.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If a search profile has unpublished changes, the list displays a warning icon (⚠️) and shows [DRAFT] after the profile's name. Publish the search profile to see these changes reflected in the search query preview.</td>
</tr>
<tr>
<td>2. Search input field</td>
<td>Enter search query terms and operators in this field. To preview the query's results using settings from the selected search profile, click <strong>Search</strong>.</td>
</tr>
<tr>
<td>3. Table facet filter</td>
<td>View the distribution of search query results by source table. To filter the query results by table, click a table's name. To remove the table facet filter, select <strong>All</strong>.</td>
</tr>
<tr>
<td>4. Genius Result answers</td>
<td>Review the key-value pairs for each Genius Result answer the search query produces when executed with the selected search profile.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Genius Result answers may not appear for all search queries.</td>
</tr>
<tr>
<td>5. Search query results</td>
<td>Review the results the search query produces when executed with the selected search profile. To page through results, click <strong>Next</strong> or <strong>Previous</strong>.</td>
</tr>
</tbody>
</table>
6. AI Search administrator tools

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6. AI Search administrator tools</td>
<td>Click the icon for the administrator tool that you want to use:</td>
</tr>
<tr>
<td></td>
<td>• Process data tool icon ( ? ) <strong>Process data</strong>: View summary information on the search query's triggered result improvement rules, matched NLU model intents, and processing time.</td>
</tr>
<tr>
<td></td>
<td>• Alerts tool icon ( ! ) <strong>Alerts</strong>: Review alert feedback messages produced during processing of the search query.</td>
</tr>
<tr>
<td></td>
<td>• Dictionary and query feedback tool icon ( ) <strong>Dictionary and query feedback</strong>: Review dictionary and query feedback messages and NLU model intent data for the search query. Enable debugging.</td>
</tr>
<tr>
<td></td>
<td>• Context settings tool icon ( ) <strong>Context settings</strong>: Specify user context values for the search query to trigger result improvement rules.</td>
</tr>
<tr>
<td></td>
<td>• User impersonation tool icon ( ) <strong>User impersonation</strong>: Change the search query's user or locale to test access settings and view translated documents.</td>
</tr>
</tbody>
</table>

For more detailed descriptions of each administrator tool's output, controls, and fields, see the following reference section.

**Search preview admin tools**

Understand the output, controls, and fields provided by admin tools in the search preview UI.

**Process data tool**

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query Rules Triggered</td>
<td>Count of result improvement rules triggered by the search query.</td>
</tr>
<tr>
<td>Intents Matched</td>
<td>Count and names of NLU model intents detected in the search query.</td>
</tr>
<tr>
<td>Total time</td>
<td>Total time spent processing the search query. Includes pre-processing, search query, Genius Result computation, and security processing times.</td>
</tr>
<tr>
<td>Pre-processing time</td>
<td>Time spent preparing the search query for execution. Includes time spent looking up the user's access permissions for content security.</td>
</tr>
<tr>
<td>Entry</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Search query time</td>
<td>Time spent retrieving records that match the search query and generating the result set.</td>
</tr>
<tr>
<td>Genius Result computation</td>
<td>Time spent computing Genius Result answers for the search query.</td>
</tr>
<tr>
<td>Security processing time</td>
<td>Time spent filtering inaccessible records out of the search query's result set based on the user's access permissions.</td>
</tr>
</tbody>
</table>

**Alerts tool**

This tool displays a list of alert feedback messages produced while processing the search query.

If the search query produced no alert feedback messages, the tool instead displays **No Alert Feedback**.

**Dictionary and query feedback tool**

This tool displays separate panes for dictionary feedback entries and query feedback controls.

**Dictionary feedback**

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stop words</td>
<td>List of feedback messages relating to stop word removal for the search query.</td>
</tr>
<tr>
<td>Spellcheck</td>
<td>List of feedback messages relating to typo handling autocorrection for the search query.</td>
</tr>
<tr>
<td>Synonyms</td>
<td>List of feedback messages relating to synonym expansion for the search query.</td>
</tr>
</tbody>
</table>

**Query feedback**

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show all feedback</td>
<td>Display a JSON array of feedback messages produced for the search query.</td>
</tr>
<tr>
<td>Show all intent data</td>
<td>Display a JSON array of NLU model intents detected in the search query.</td>
</tr>
<tr>
<td>Debug</td>
<td>Enable this option to set <code>sysparm_debug</code> to <code>true</code> when submitting search preview queries.</td>
</tr>
</tbody>
</table>

**Note:** To use this tool, you must have the impersonator role.
Context settings tool

With these tools, you can specify user context values to test user context triggers for result improvement rules.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Domain</td>
<td>To set a domain in the user context for search preview, enter the name of a group from the Group [sys_user_group] table.</td>
</tr>
<tr>
<td>User Company</td>
<td>To set a company in the user context for search preview, enter the name of a company from the Company [core_company] table.</td>
</tr>
<tr>
<td>User Office</td>
<td>To set an office in the user context for search preview, enter the name of a building from the Building [cmn_building] table.</td>
</tr>
<tr>
<td>User Department</td>
<td>To set a department in the user context for search preview, enter the name of a department from the Department [cmn_department] table.</td>
</tr>
<tr>
<td>User Title</td>
<td>To set a title in the user context for search preview, select it from the list. This list includes all Title values found in the User [sys_user] table.</td>
</tr>
<tr>
<td>User Location</td>
<td>To set a location in the user context for search preview, enter the name of a location from the Location [cmn_location] table.</td>
</tr>
<tr>
<td>User Role</td>
<td>To set a role in the user context for search preview, enter the name of a role from the Role [sys_user_role] table.</td>
</tr>
<tr>
<td>User Country</td>
<td>To set a country in the user context for search preview, select it from the list. This list includes all countries found in user locations from the User [sys_user] table.</td>
</tr>
<tr>
<td>User Language</td>
<td>To set a language in the user context for search preview, select it from the list of supported languages.</td>
</tr>
<tr>
<td>User Office Country</td>
<td>To set an office country in the user context for search preview, select it from the list. This list includes all countries found in user locations from the User [sys_user] table.</td>
</tr>
<tr>
<td>User Office City</td>
<td>To set an office city in the user context for search preview, enter it in this field. You can enable session debugging for AI Search to review values submitted for this user context field in user queries.</td>
</tr>
<tr>
<td>User Office State</td>
<td>To set an office state in the user context for search preview, enter it in this field. You can enable session debugging for AI Search to review values submitted for this user context field in user queries.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User OS</td>
<td>To set an operating system in the user context for search preview, enter its name in this field. You can enable session debugging for AI Search to review values submitted for this user context field in user queries.</td>
</tr>
<tr>
<td>User Device Type</td>
<td>To set a user device type in the user context for search preview, enter it in this field. You can enable session debugging for AI Search to review values submitted for this user context field in user queries.</td>
</tr>
<tr>
<td>User OS Version Type</td>
<td>To set an operating system version type in the user context for search preview, enter it in this field. You can enable session debugging for AI Search to review values submitted for this user context field in user queries.</td>
</tr>
<tr>
<td>User Browser Agent</td>
<td>To set a browser agent string in the user context for search preview, enter it in this field. You can enable session debugging for AI Search to review values submitted for this user context field in user queries.</td>
</tr>
<tr>
<td>User Browser</td>
<td>To set a browser name in the user context for search preview, enter it in this field. You can enable session debugging for AI Search to review values submitted for this user context field in user queries.</td>
</tr>
<tr>
<td>User Device Form</td>
<td>To set a device form in the user context for search preview, enter it in this field. You can enable session debugging for AI Search to review values submitted for this user context field in user queries.</td>
</tr>
</tbody>
</table>

**User impersonation tool**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search as</td>
<td>To submit search preview queries as another user, enter the user's name from the User [sys_users] table. You must have the impersonator role. Use this control to see how content security affects search query results for specific user accounts.</td>
</tr>
</tbody>
</table>

**Note:** Searches performed while impersonating another user do not affect the Search users metric, trend, and report on the Search Analytics dashboard.

| Query Locale | To submit search preview queries using a specific supported language, select the language from the list. Use this control to observe differences in search query results for different languages. |
**Contextual search**

Contextual search is a search technology that focuses on the context of the query as well as the intent of the user in order to fetch the most relevant set of results. Contextual search displays related results within a form or record producer based on the text you enter in a field.

Example use cases for Incident:

- An agent, working on an Incident record, can use contextual search to find and attach knowledge articles, order a catalog item on behalf of the caller, or search for an article and link it to a related incident or problem.
- A user, creating an Incident via the Service Portal, can see related catalog items that the user can order. The user can also view related knowledge articles to help them resolve the issue on their own without involving the service desk operators.

Contextual search helps with incident deflection for the following areas:

- Incident record producers: deflecting incidents by helping end users resolve issues before they raise an incident.
- Incident forms: helping service desk staff resolve incidents quickly by providing relevant knowledge.
- Incident email notifications: helping end users resolve their incidents themselves without requiring manual intervention from service desk staff.

**Contextual search plugin**

Contextual search plugin is activated in the base system.

**Contextual search plugin**

The Contextual Search plugin (com.snc.contextual_search) is activated by default in the base system. This plugin activates related plugins if they are not already active.

If the related plugins are not activated, Contextual Search activates the plugins.

<table>
<thead>
<tr>
<th><strong>Plugins for Contextual Search</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Contextual Search — Internal [com.snc.contextual_search.internal]</td>
<td>An internal plugin component for Contextual Search.</td>
</tr>
<tr>
<td>GraphQL Schema for Contextual Search [com.snc.contextual_search.graphql]</td>
<td>Provides GraphQL schema for contextual search services.</td>
</tr>
</tbody>
</table>

1. Navigate to System Applications > All Available Applications > All.
2. Find the plugin using the filter criteria and search bar.
   
   You can search for the plugin by its name or ID. If you cannot find a plugin, you might have to request it from ServiceNow personnel. For more information, see Request a plugin.
3. Click Install, and then in the Activate Plugin dialog box, click Activate.

**Note:** When domain separation and delegated admin are enabled in an instance, the administrative user must be in the **global** domain. Otherwise, the following error appears: Application...
Components installed with Contextual Search
Several types of components are installed with the activation of the Contextual Search plugin (com.snc.contextual_search), including tables and user roles.

Note: The Application Files table lists the components that are installed with this application. For instructions on how to access this table, see Find components installed with an application.

Tables installed

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available Search Resource</td>
<td>List of available search resources used in configuration of searches.</td>
</tr>
<tr>
<td>[cxs_search_resource]</td>
<td></td>
</tr>
<tr>
<td>Email Configuration</td>
<td>List of email notifications configured to have contextual search results attached.</td>
</tr>
<tr>
<td>[cxs_table_email_config]</td>
<td></td>
</tr>
<tr>
<td>Record Producer Configuration</td>
<td>List of record producers configured to have contextual search.</td>
</tr>
<tr>
<td>[cxs_rp_config]</td>
<td></td>
</tr>
<tr>
<td>Relevant Document</td>
<td>Groups the Relevant Document Detail individual recorded actions by search session.</td>
</tr>
<tr>
<td>[cxs_relevant_doc]</td>
<td></td>
</tr>
<tr>
<td>Relevant Document Detail</td>
<td>List of individual recorded actions. For example, Preview, This helped, Attach, or Order. For more information on the table, refer Feedback information on contextual search.</td>
</tr>
<tr>
<td>[cxs_rel_doc_detail]</td>
<td></td>
</tr>
<tr>
<td>Search Context</td>
<td>Search contexts for contextual search.</td>
</tr>
<tr>
<td>[cxs_context_config]</td>
<td></td>
</tr>
<tr>
<td>Search Field</td>
<td>All form fields that have contextual search configured to it.</td>
</tr>
<tr>
<td>[cxs_table_field_config]</td>
<td></td>
</tr>
<tr>
<td>Search Resource</td>
<td>Search resource configurations for the related searcher.</td>
</tr>
<tr>
<td>[cxs_search_res_config]</td>
<td></td>
</tr>
<tr>
<td>Search Resource Context Configuration</td>
<td>Conditions for this search context that restrict the results returned to a user.</td>
</tr>
<tr>
<td>[cxs_res_context_config]</td>
<td></td>
</tr>
</tbody>
</table>
### Contextual search concepts

Contextual search concepts help you to understand different contextual search components that are used in the documentation, configuration, and user interface. Understanding of the concepts makes it easier for you to comprehend the interconnection between the components.

Contextual search uses terms and concepts that can differ from industry norms due to the unique nature of the ServiceNow platform. Contextual search includes the following concepts and components:

**Search resource**

Resource that can be searched such as Catalog or Knowledge Articles. As the resources are scripted and contain JavaScript, they can combine results from more than one table.

**Note:**

- ServiceNow provides pre-defined scripted search resources. You cannot create, update, or delete search resources.
- A search resource uses the Zing search engine to search a table.

**Searcher**

A single search resource or a group of search resources that can be searched. For example, the Knowledge and catalog searcher contains Knowledge Articles, Questions and Catalog Items as its search resources.

**Note:** ServiceNow provides pre-defined searchers. You cannot create, update, or delete searchers.

**Additional resources**

An additional resource is a single table source with query conditions that you can search. Additional resource are not scripted as you search from a single table. For example, Resolved Incidents (within the last six months).

**Note:**

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Resource Context Property</td>
<td>Property values for search resource context configuration.</td>
</tr>
<tr>
<td>[cxs_res_context_config_prop]</td>
<td></td>
</tr>
<tr>
<td>Search Resource Property</td>
<td>Property values for search resource searcher configuration.</td>
</tr>
<tr>
<td>[cxs_search_res_config_prop]</td>
<td></td>
</tr>
<tr>
<td>Searcher Configuration</td>
<td>Details of available search configurations.</td>
</tr>
<tr>
<td>[cxs_searcher_config]</td>
<td></td>
</tr>
<tr>
<td>Table Configuration</td>
<td>Lists the tables configured for table configurations.</td>
</tr>
<tr>
<td>[cxs_table_config]</td>
<td></td>
</tr>
<tr>
<td>Wizard Configuration</td>
<td>Lists the tables configured for wizard configurations.</td>
</tr>
<tr>
<td>[cxs_wizard_config]</td>
<td></td>
</tr>
<tr>
<td>Base UI Configuration</td>
<td>Common elements for the record producer, table, and wizard configurations.</td>
</tr>
<tr>
<td>[cxs_ui_config_base]</td>
<td></td>
</tr>
</tbody>
</table>
• ServiceNow provides pre-defined additional resources. You cannot create or delete additional resources, but can update additional resources to better match your organization requirements. For example, you can update the condition and description for Resolved Incidents (Last 6 months) to change it to Resolved Incidents (Last 3 months).
• An additional resource performs the search based on the type of the source:
  • Table: The Zing search engine to used to search a table.
  • Predictive Intelligence Similarity: Search is based on similarity and not on the Zing search engine.

Search result display fields

Defines the fields whose values are displayed with the search result of an additional resource. The fields can include Assigned to, Opened by, and State. The search result display fields appear at the bottom of a search result record.

**Note:** ServiceNow provides pre-defined search result display fields. You cannot create or delete additional resources, but you can update search result display fields to better match your organization requirements. For example, change which field to use as a title or the description or which fields to show at the bottom of a search result record.

Search context

Brings together a searcher and additional resources (if any) that can be searched.

**Note:** ServiceNow provides pre-defined search contexts. You can also create search contexts.

Searcher text

Defined in a search context, a searcher text specifies a user-friendly group name for the searcher. When a searcher contains more than one search resource, a group name is used to represent that group of search resources. For example, the Incident Deflection search context uses a searcher that searches Knowledge Articles, Questions and Catalog Items. The user-friendly searcher group name that represents all of them is Knowledge & Catalog.

Search on tab

Defined in the search context, Search on tab specifies when a contextual search should start the search. The different scenarios when search is performed are:

- If you select the Search on tab check box, the search only runs when you update and leave the search field (recommended).
- If you clear the Search on tab check box, the search runs when you pause typing.

Search actions

Specifies the actions for each such results. For example, for catalog items, the search action is Order and for knowledge articles it is Attach. All sources have the This helped action.
Contextual search components diagram

The contextual search components diagram helps you to understand how contextual search concepts work together to perform a search and from which module you can configure the components.
You can configure the search header text and the form using the Contextual search > Table configuration module. For more information, refer Configure table for a contextual search.

You can configure the searcher text and the searcher using the Contextual search > Search Contexts module. For more information, see Define a search context.
Components

<table>
<thead>
<tr>
<th>Search Result Display Configurations</th>
<th>Navigation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>You can configure the card title, card description field, and card additional fields using the Contextual search &gt; Search Result Display Configurations module. For more information, see Edit search resource display field record.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Search Action Configurations</th>
<th>Navigation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>You can configure the search actions using the Contextual search &gt; Table Configuration &gt; Search Action Configurations module. For more information, see Modify or disable search actions available for contextual search.</td>
</tr>
</tbody>
</table>

Configuring contextual search

You can configure different components of contextual search.

Contextual search properties

Contextual search properties are used to control the fields that you can search from and the number of results displayed per page.

The contextual search properties are available at Contextual Search > Properties.

Properties for contextual search

<table>
<thead>
<tr>
<th>Property label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default value for maximum number of search results returned for table and record producer configurations</td>
<td>Default value for the maximum number of search results returned when you create a new table or record producer configuration. By default, the value is 10.</td>
</tr>
<tr>
<td>[com.snc.contextual_search.result.default.limit]</td>
<td></td>
</tr>
</tbody>
</table>

| Number of characters that a configured field needs before triggering a search | Number of characters that contextual search requires before triggering a search based on the typed text in the search field. By default, the value is set to 3 characters. |
| [com.snc.contextual_search.min_length] | |

| Number of milliseconds that a configured field will wait before triggering a search | Number of milliseconds that contextual search waits before triggering a search based on the typed text in the search field. By default, the value is set to 1,000 milliseconds (one second). |
| [com.snc.contextual_search.wait_time] | |

<p>| Records returned above this threshold will log warnings | Triggers a warning message within the system log whenever more than this number of results are returned in a search. This logging helps if you are experiencing performance issues because of large searches. By default, the value is set to 10,000 results. |
| [com.snc.contextual_search.result.threshold] | |</p>
<table>
<thead>
<tr>
<th>Property label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>When a Form configuration is created a search field with a name matching this property will be automatically created</td>
<td>The default field that is used for searching when you create a new table configuration. By default, the value is set to short_description.</td>
</tr>
<tr>
<td>[com.snc.contextual_search.widget.form.default_field]</td>
<td></td>
</tr>
<tr>
<td>Collapse the search results widget when creating a new record in a form</td>
<td>When the value is set to false and you create a new record, the search results widget is collapsed to save space. By default, the value is set to false.</td>
</tr>
<tr>
<td>[com.snc.contextual_search.widget.form.open_collapsed_new_records]</td>
<td></td>
</tr>
<tr>
<td>Collapse the search results widget when opening an existing record in a form</td>
<td>When the value is set to true and you open an existing record, the search results widget is collapsed to save space. By default, the value is set to true.</td>
</tr>
<tr>
<td>[com.snc.contextual_search.widget.form.open_collapsed_existing_records]</td>
<td></td>
</tr>
<tr>
<td>Auto expand the search results widget when search field updates in a form</td>
<td>When the value is set to true and the search results widget stays collapsed until you click the search results widget to expand it manually. By default, the value is set to true.</td>
</tr>
<tr>
<td>[com.snc.contextual_search.widget.form.expand_on_search_field_update]</td>
<td></td>
</tr>
<tr>
<td>Show meta data on form contextual search results</td>
<td>When the value is set to true, each search result includes additional meta data below each result record. By default, the property is set to true.</td>
</tr>
<tr>
<td>[com.snc.contextual_search.widget.form.show_meta_data]</td>
<td></td>
</tr>
</tbody>
</table>

**Define a search context**

Define a search context to configure relevant resources based on your business needs. For example, you can show different resources for an agent working on an Incident and different resources for a problem co-ordinator working on a Problem. The search resources can be pre-defined resources as well as additional resources.

Role required: admin

1. Navigate to Contextual Search > Search Contexts.
2. Click New.
3. On the form, fill in the fields.

![Search Context form](image)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name of the search context.</td>
</tr>
<tr>
<td>Short description</td>
<td>Brief summary of the context.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Searcher</td>
<td>Lookup icon to select a searcher for this context. The searcher determines the information source to search.</td>
</tr>
<tr>
<td></td>
<td>• Catalog only: Provides search results from service catalog items.</td>
</tr>
<tr>
<td></td>
<td>• Knowledge and catalog: Provides search results from knowledge articles and service catalog items.</td>
</tr>
<tr>
<td></td>
<td>• Knowledge only: Provides search results from knowledge articles.</td>
</tr>
<tr>
<td></td>
<td>• Knowledge, Discussions and pinned: Provides search results from knowledge articles, pinned knowledge articles and Now Community.</td>
</tr>
<tr>
<td></td>
<td>• Knowledge, pinned knowledge and catalog: Provides search results from knowledge articles, pinned knowledge articles and service catalog items.</td>
</tr>
<tr>
<td></td>
<td>• Knowledge and pinned knowledge: Searches knowledge articles and pinned knowledge articles.</td>
</tr>
<tr>
<td></td>
<td>• Knowledge, Pinned, Catalog: Provides search results from Knowledge, Pinned Knowledge, and Catalog items.</td>
</tr>
<tr>
<td></td>
<td>• Knowledge and pinned: Provides search results from knowledge articles and pinned knowledge articles.</td>
</tr>
<tr>
<td></td>
<td>• Pinned Knowledge only: Provides search results from pinned knowledge articles.</td>
</tr>
</tbody>
</table>

**Note:** The **Searcher** field is optional. You can decide whether to show or hide sources from an agent.

<table>
<thead>
<tr>
<th>Searcher text</th>
<th>Unique label for the searcher group that is used when there is more than one resource in the searcher.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Check box to activate the search context form.</td>
</tr>
<tr>
<td>Enable wildcard searches</td>
<td>Check box to enable wildcard characters, such as * and %, for searches.</td>
</tr>
<tr>
<td>Search on tab</td>
<td>Check box to determine when to perform the search. If you select this option, the search runs only when you enter text in a field and then leave the field. If you clear the check box, the search runs after you stop typing even though the cursor is still in the same field.</td>
</tr>
</tbody>
</table>

**Note:** Ensure you select the check box to see additional resources in the source selector on Platform.

4. Right-click the form header and click **Save**.
Configure table for a contextual search

Configure the search that is performed and the actions that you can take on the search result for the table.

Role required: admin

1. Navigate to Contextual Search > Table Configuration and click New.
2. On the form, fill in the fields.
### Table Configuration fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>Name and label of the table associated with the form. For example, Incident [incident].</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>UI type</td>
<td>User interface differs depending on whether you use the table configuration for Platform or Workspace.</td>
</tr>
</tbody>
</table>

**Note:** The *When to display* section appears only when you select **Platform** from **UI type**.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show searcher first</td>
<td>Option to display searcher resources before additional resources in the search context. This field appears only when you select <strong>Workspace</strong> from <strong>UI type</strong>.</td>
</tr>
<tr>
<td>Search context</td>
<td>Lookup icon</td>
</tr>
<tr>
<td></td>
<td>to select a search context for which you are configuring the table.</td>
</tr>
<tr>
<td>Results header text</td>
<td>Unique name that appears as a header for the search results area that appears in the form. For example, if you enter <strong>Knowledge results</strong> as the value in this field, the related search area displays <strong>Knowledge results</strong> as the name.</td>
</tr>
<tr>
<td>Enable related search box</td>
<td>Option to show the related search box in the form.</td>
</tr>
<tr>
<td>Enable source selector</td>
<td>Option to show the list of search sources that you can search from.</td>
</tr>
<tr>
<td>Application</td>
<td>Application scope of the table configuration. The configuration is available for all applications or for scoped applications.</td>
</tr>
<tr>
<td>Active</td>
<td>Option to activate the table configuration.</td>
</tr>
<tr>
<td>Limit</td>
<td>Maximum number of search results returned.</td>
</tr>
<tr>
<td>Results per page</td>
<td>Number of results to display per page.</td>
</tr>
<tr>
<td>Allow expand/collapse</td>
<td>Option to enable a user to collapse the search results in the form.</td>
</tr>
<tr>
<td>Enable preview buttons</td>
<td>Option to show a preview button (platform only) for each search result. The user can then use the preview button or the search result title to preview the result record.</td>
</tr>
</tbody>
</table>

**Note:** This field appears only when you select **Enable related search box**.

**Note:** The option is available from the London release. Clear the option to provide a more compact display for each search result.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow search with empty search text</td>
<td>Option to specify whether the search runs when there is no search text.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>There is no search text when there is no search field specified or when there is a search field whose value is empty.</td>
</tr>
<tr>
<td>When to display</td>
<td></td>
</tr>
<tr>
<td>Required roles</td>
<td>List of roles that grant access to the related search results widget from the table. Users must have one of these roles to see the widget when viewing the table.</td>
</tr>
<tr>
<td>Condition</td>
<td>Conditions that records must satisfy to appear as related search results. For example, set <strong>[Active] [is] [true]</strong> to only enable the active records as related search results.</td>
</tr>
<tr>
<td>Search as</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable search as</td>
<td>Option to enable searching as a different user. The message box describes the settings available when you select this.</td>
</tr>
</tbody>
</table>
3. Click **Submit**.
   The Search Fields, Filter Configurations, Email Configurations, and Search Action Configurations related lists appear. By default, the **Short description** field is added to the Search Fields related list.

**Filter configuration for contextual search**

Define filter configurations to map fields from the form to provide a more targeted search result set. 

*Create a filter configuration using mapping*

Create filter conditions using mapping that you can associate with a table configuration. The search result displays result that meets the filter conditions.

Role required: admin

1. Navigate to **Contextual Search > Table Configuration**.
2. Open a table configuration record on which to create the filter.
3. In the Filter Configurations related list, click **New**.
4. On the form, fill in the fields.

**Filter Configuration form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Resource configuration | Lookup icon  
|                   | to select a resource such as Knowledge Articles.                           |
| Table configuration | [Read-only field]. Table for which you are applying the filter configuration. |
| Scripted filter   | Check box to select if you want to enter scripts in the **Script** field.    |
| Note: Clear the check box as you want to create a filter configuration using mapping. |
| Active            | Check box to activate the filter configuration.                             |

5. Click **Submit**.
   The Table Configurations form appears.

6. In the Filter Configuration related list, click the filter that you have created.
7. In the Filter Conditions related list, click **New**.

![FilterConditions.png](image)

8. In the form, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short description</td>
<td>Brief summary of the filter condition.</td>
</tr>
<tr>
<td>Query table</td>
<td>[Read-only] Table from which the filter condition is queried.</td>
</tr>
<tr>
<td>Current form</td>
<td>[Read-only] Form for which you created the filter conditions.</td>
</tr>
<tr>
<td>Field to compare</td>
<td>Value of the field is compared with the value of the <strong>Compare to</strong> field.</td>
</tr>
<tr>
<td>Operator</td>
<td>Operation that should be performed on the <strong>Field to compare</strong> and <strong>Compare to</strong> field.</td>
</tr>
<tr>
<td>Compare to</td>
<td>Value of the field is compared against the value of <strong>Field to compare</strong>.</td>
</tr>
<tr>
<td>Compare</td>
<td>Comparison of the field can be based on the actual value stored on the database or the value that is displayed on the interface. The available values are: <strong>Value</strong> and <strong>Display Value</strong>.</td>
</tr>
<tr>
<td>Include if blank</td>
<td>Check box to include a condition when the value of the <strong>Compare to</strong> field is blank.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box to activate the filter configuration.</td>
</tr>
</tbody>
</table>

9. Click **Submit**.

*Create a filter configuration using scripts*

Create filter conditions using script that you can associate with a table configuration. The search result displays results that meet the filter conditions.

Role required: admin

1. Navigate to **Contextual Search > Table Configuration**.
2. Open a table configuration record on which to create the filter.
3. In the Filter Configurations related list, click **New**.
4. On the form, fill in the fields.

**Filter Configuration form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource configuration</td>
<td>Lookup icon to select a resource such as Knowledge Articles.</td>
</tr>
<tr>
<td>Table configuration</td>
<td>[Read-only field]. Table for which you want to apply the filter configuration.</td>
</tr>
<tr>
<td>Scripted filter</td>
<td>Check box to select if you want to enter scripts in the Script field.</td>
</tr>
<tr>
<td>Application</td>
<td>Application scope for your filter configuration.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box to activate the filter configuration.</td>
</tr>
</tbody>
</table>

5. Enter a script corresponding to the resource configuration.

**Note:**

Use one of these dynamic filter scripts to set up your dynamic filter.

6. Click Submit.

**Configure search resource context properties**

Configure the properties to limit the search to a specific catalog or knowledge base. For example, if you want to limit the knowledge search to an IT knowledge base or a service catalog search to software service catalog, you can configure the properties.

Role required: admin

The following procedure uses Incident Deflection as an example.

1. Navigate to **Contextual Search > Search Contexts**.
2. Open the Incident Deflection record.
3. Click the Resource Configurations related list.

In the Resource Configurations related list, click a resource configuration record to know the properties of the search resource.

The **knowledge** record displays the following knowledge resource configuration properties:

<table>
<thead>
<tr>
<th><strong>Property</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition</td>
<td>Conditions to specify one or more knowledge bases to search.</td>
</tr>
<tr>
<td>Exclude pinned articles</td>
<td>Pinned article is a knowledge article. This property helps to decide whether to exclude pinned articles from knowledge base search or not.</td>
</tr>
</tbody>
</table>

The **catalog** record displays the following catalog resource configuration properties:

<table>
<thead>
<tr>
<th><strong>Property</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalog name</td>
<td>A catalog name to search the catalog items.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Search operator  | Value of the operator is used in the Zing search engine to instruct how to combine the AND and OR conditions when parsing the search string. The integration of the search strings helps to score the displayed results. The value can only be one of the following values:  
  - **IR_AND_OR_QUERY** (the default): Display results with exact matches of all terms if the number of results is greater than the value of the `glide.ts.query.and_or_limit` property (default 0) or the (overriding) value of the table custom attribute `text_search_and_or_limit` (when added). Otherwise display results with any matches of any terms.  
  - **IR_AND_QUERY**: Display results with exact matches of all terms only.  
  - **IR_OR_QUERY**: Display results with any matches of any terms.                                                                                                    |

4. To edit the value of any property, click the property name and in the Search Resource Context Property form, update the **Value** field to **true** or **false**.

5. Click **Update**.

**Managing contextual search**

Contextual search provides a way to display results that can be relevant to the issue for which you are creating an incident or requesting a service.

The section covers topics that help you to:

- Understand the actions that are taken on the search results.
• Use contextual search results in a record producer within the Service Portal or as an agent in a form.

Set a search context as default

If you use the contextual search REST API and do not specify which search context to use, the API uses the search context that you have set as default. The search context that you use in the API takes preference over the one marked as default.

Role required: admin

1. Navigate to **Contextual Search > Search Contexts.**
2. Open the search context record that you want to set as default.
3. Click **Set As Default**.
Set default source for search context

You can decide if you want an additional resource to be the default source or the searcher.

Role required: admin

- If you set an additional resource as default that is considered as the default source.
- If you do not mark any additional resource as default, then the searcher is considered as the default source.
- If you do not have a searcher and you have not marked any additional resource as default, the default is the additional resource with the lowest value in the `Order` field.

1. Navigate to **Contextual Search > Search Contexts.**
2. Open the search context record to change its default source.
3. Click the Additional Resource Configuration related list.

4. Click the preview information icon to the left of the search resource configuration record and click **Open Record.**
5. Click **Set As Default.**

**Note:** If you want to remove the default value, click **Clear Default.**
**View a searcher**

View the details of a searcher to know which search resources are searched.

Role required: admin

ServiceNow provides pre-defined searchers. You cannot create, update, or delete searchers.

1. Navigate to **Contextual Search > Searchers**.
2. Open a searcher record.

![Searcher configuration](image)

3. Optional: In the Search Resources related list, view which search resources are searched.
4. Optional: In the Search Contexts related list, view all the search contexts that use this specific searcher.

**Show related search box in a form**

Show the related search box when you want the agent to search for different text without having to modify the text in the **Short description** field.
Role required: admin

From the London release, the related search box is available in the forms by default for the new customers. In case you do not find the related search box for any form, you can always configure the table for the same.

1. Navigate to **Contextual Search > Table Configuration**.
2. Open the table record for which you want to show the related search box.
3. Select the **Enable related search box** check box.
   The **Enable source selector** check box appears.
4. Right-click the header form and select **Save**.

### Add multiple search fields for contextual search

Add multiple search fields if you want to search from a field other than the short description without using the related search box.

Role required: admin

Search results for the default search field appear automatically when you open a record. You can configure contextual search to search for results even when there is no text in the search field. Search results in other associated fields only appear when you have updated content in those fields. For example, in the base system the **Short description** field is the default search field for the Incident form, so search results based on the field are displayed automatically. If there are multiple fields, the search is conducted based on the last updated field.

1. Navigate to **Contextual Search > Table Configuration**.
2. Open the table record for which you want to add multiple search fields.
3. In the Search fields related list, click **New**.
4. On the form, fill in the fields.

![Search Field form](image)

**Search Field form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
<td>The search field to be added in the search fields list.</td>
</tr>
</tbody>
</table>

**Note**: You can only select a text field.
5. Click **Submit**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Application scope of the table configuration. The configuration is available for all applications or for scoped applications.</td>
</tr>
<tr>
<td>Order</td>
<td>Order in which the field appears in the search fields list. If there are multiple search fields, this field indicates which searched field is executed first.</td>
</tr>
</tbody>
</table>

Use the **Default** column to set any field as the default one.

**Add additional resources to the source selector of a form**

Add additional resources when you want the user to search beyond knowledge and service catalog search resources. For example, add additional resources for **Open Incidents**, **Resolved Incidents** or **Similar Open Incidents**.

Role required: admin

Additional resources are pre-defined. An additional resource is a single source table with query conditions that can be searched or they can reference a Predictive Intelligence Similarity solution definition.

You can view the Predictive Intelligence sources only if you are licensed for Predictive Intelligence and have activated **Predictive Intelligence for Contextual Search**

1. Navigate to **Contextual Search > Search Contexts**.
2. Open the search context record for which you want to see the additional resources.
3. In the Additional Resource Configurations related list, click **Edit**.
4. From the Collection field, move the required additional resources to the Additional Resource Configurations List field.

For example, if you want to move additional resources whose type is Predictive Intelligence Similarity, then move Similar Incidents, Similar Knowledge Articles, Similar Open Incidents, and Similar Resolved Incidents from the Collection field to the Additional Resource Configurations List field.

Note: You can view the Predictive Intelligence sources only if you have license for Predictive Intelligence.
5. Click **Save**.

The search resources appear under **Additional Resource Configurations**.

![Additional Resource Configurations Table]

---

**Edit search resource display field record**

Use the search result display fields to provide title, description, and additional information about the search result.

Role required: admin

ServiceNow provides pre-defined additional resource or search sources to the user. You cannot create or delete search result display configurations. Each table referred by an additional resource has a search result display configuration record. You can edit the values in the **Card title field**, **Card description field**, and the **Card additional fields**.
Note: Ensure that you select the contextual search property **Shows meta data on form contextual search results** to view **Card additional fields** in the search result.

1. Navigate to **Contextual Search > Search Result Display Configurations**.
2. Open the search result display configuration record that you want to modify.
3. In the form, edit the fields.

### Search Result Fields form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UI type</td>
<td>[Read-only] Interface where the values of the search result display fields should appear. It can appear in platform or workspace.</td>
</tr>
<tr>
<td>Table</td>
<td>[Read-only] Name of the table in which the values of the search result display fields should appear. For example, if you mention Incident [incident] as the table, then the additional resource field values appear in the search result for the Incident [incident] table.</td>
</tr>
<tr>
<td>Application</td>
<td>[Read-only] Application scope of the record. The record is available for all applications or for scoped applications.</td>
</tr>
<tr>
<td>Card View</td>
<td></td>
</tr>
<tr>
<td>Card icon</td>
<td>[Workspace] Icon name displayed on the search result card view.</td>
</tr>
<tr>
<td>Card label</td>
<td>[Workspace] Label displayed on the search result card view.</td>
</tr>
<tr>
<td>Card title field</td>
<td>[Platform or Workspace] Field whose value is shown as title in the search result title.</td>
</tr>
<tr>
<td>Card additional fields</td>
<td>[Platform or Workspace] List of field names displayed on the search result to provide more context to the search result. The card additional fields appear at the bottom of a search result record.</td>
</tr>
<tr>
<td>Card description field</td>
<td>[Platform or Workspace] Name of the field whose value is shown as the search result description.</td>
</tr>
<tr>
<td>Card display updated date</td>
<td>[Workspace] Check box to display the latest date on the search result card view.</td>
</tr>
<tr>
<td>Details View (only when the UI type is Workspace)</td>
<td></td>
</tr>
<tr>
<td>Detail title field</td>
<td>Field whose value is shown as title in the search result detail view.</td>
</tr>
<tr>
<td>Detail link field</td>
<td>Field used as clickable link on the search result detail view.</td>
</tr>
<tr>
<td>Detail additional fields</td>
<td>List of field names displayed on the search result detail view.</td>
</tr>
<tr>
<td>Detail show last work note</td>
<td>Check box to display the latest work note on the search result detail view.</td>
</tr>
</tbody>
</table>

4. Click **Update**.

### Specify fields for the Cxs_popup view

Edit the Cxs_popup view to specify the fields to be shown for addition resources in the preview window of a task record. The preview helps you with the summary of the record.

Role required: admin
If a Cxs_popup view is not defined for the additional resource table, the sys_popup view is used. If the sys_popup view is also not defined, the default view is considered.

1. Navigate to **Incident > All**.
2. Open the incident record whose view you want to change to Cxs_popup.
3. Click the additional actions icon ( ) and in the View option, click **Cxs_popup**.

The view of the incident record changes to **Cxs_popup** view.
4. Click the additional actions icon ( ), and in the Configure option, select Form Layout.

5. From the Available list of fields, select the fields that you want to be available in the Cxs_popup view and move them under Selected.

6. Click Save.

Modify or disable search actions available for contextual search

Modify or disable search actions to restrict the actions that a user can perform on a search result.

Role required: admin

The Search Action Configurations related list contains all the available Search actions available for the selected Search context. Search actions can be modified and disabled but not deleted and new actions cannot be created.

1. Navigate to Contextual Search > Table Configuration.

2. Open a record.
3. In the Search Action Configurations related list, view the list of search actions available for the contextual search.

<table>
<thead>
<tr>
<th>Action label</th>
<th>Attachment type</th>
<th>Show on new record</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order</td>
<td>ServiceCreateSearchResource</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>This helped</td>
<td>Helpful</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>This helped</td>
<td>HelpdeskSearchSearchResource</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>This helped</td>
<td>HelpdeskSearchSearchResource</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>Attach</td>
<td>Embedded link to article</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>This helped</td>
<td>ServiceCreateSearchResource</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>Link to incident</td>
<td>HelpdeskSearchSearchResource</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>Link to incident</td>
<td>HelpdeskSearchSearchResource</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>Link to incident</td>
<td>HelpdeskSearchSearchResource</td>
<td>true</td>
<td>true</td>
</tr>
</tbody>
</table>

To disable a search action, set the value of **Active** to **false**.

**Note:** You cannot disable the **This helped** action.

The search actions that you can modify are as follows:

- **Action label**: Label on the action button on the preview window. For example, **This helped** or **Attached To Incident**.
- **Attachment type**: Method to attach a knowledge article with the record. You can embed a link (recommended) to the article or embed a copy of the article.
- **Show on new record**: Enables the **Attach** button to appear when you are creating a record. Prior to the London release, the user had to fill out and save the form, then re-expand the related search results to access the **Attach** button.
Note: This option only applies to tables with the Platform UI type. It defaults to false to provide a consistent user experience between Platform and Workspace tables.
Getting Around in Windows

Windows 8.x

Windows 8.x is designed for using touch, mouse, and keyboard together, on hardware ranging from touch-enabled tablets and laptops to PCs and all-in-one computers, including those without touch capability.

Start screen and Desktop

- 8.1: Microsoft updated the Windows 8.1 interface by returning the Start button, providing ease of access along with the option of the Metro interface. The intent is to provide a seamless experience on desktops, laptops, tablets, and phone devices.
  
  By default, the Start screen is displayed. Move your mouse pointer to the bottom left corner of the screen to make the Start button appear.
  
  Click it to display the desktop; click it again to display the Start screen.

- 8: The Start screen has a default application display you can customize:

  1. Right-click any app and the Application bar will appear at the bottom, with options for the application you selected.
  
  2. To add an app to the Start screen, click Pin to Start.

  If an application is already on the Start screen, you’ll see Unpin from Start instead.
Enable viewing of search results for the current and another selected user

Enable the search as functionality when you want the user to be able to view the search result based on what is common for both the user as well as another user.

Role required: admin

For example, an HR administrator may have some confidential information. A user might have partial access to the information. The Search as functionality applies security access to display results that are common to both the logged in or current user and the user referenced in the Search as field. The search result for the other user may have fewer entries than what that current user can actually view.

Note: No search result is displayed for the Predictive Intelligence Similarity additional resource. Record producers only support searching for the current user.

1. Navigate to Contextual Search > Table Configuration.
2. Open a table configuration record.
3. In the Search as section, fill in the fields.
When enabled, Search As displays the search results that appear for the user defined in the Search As field.

Results appear in a separate tab next to the search results the current user sees.

Use Condition and Script to restrict when the other user's results appear. Results appear if both checks evaluate to true:

- Condition in the Condition field evaluates to true, or the condition is empty.
- The script in the Script field evaluates to true, or sets the variable "answer" to true, or is empty.

Enable search as

Search as field

Assigned to

Results message

Some results may not be displayed due to security constraints

Condition

Add filter condition

Add "OR" clause

- Choose field --
- oper --
- value --

Script

1
### Search as configuration fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable search as</td>
<td>Option to enable the Search as functionality.</td>
</tr>
<tr>
<td>Search as field</td>
<td>Field defining the other user to search as. This field appears only when you select <strong>Enable search as</strong>.</td>
</tr>
<tr>
<td>Results message</td>
<td>Message to display with search results when searching as a different user. This field appears only when you select <strong>Enable search as</strong>.</td>
</tr>
<tr>
<td>Condition</td>
<td>Condition restricting when the search result of the user mentioned in the <strong>Search as field</strong> should appear. This field appears only when you select <strong>Enable search as</strong>.</td>
</tr>
<tr>
<td>Script</td>
<td>A condition script, enabling administrators to implement more powerful conditions. For example, to restrict access to users that are members of a group, use <code>gs.getUser().isMemberOf(&quot;&lt;group name&gt;&quot;)</code>. This field appears only when you select <strong>Enable search as</strong>.</td>
</tr>
</tbody>
</table>

**Note:** Both **Condition** and **Script** must evaluate to **true** for search results to appear. An empty condition or script also evaluates to **true**.

The **My Results** tab displays the search result for the current user. The **<User name>’s results** tab displays the search result for the user referenced in the **Search as field**.

### Define contextual search for record producer

Define a record producer to trigger a search based on the text that you enter in a variable field. Search results appear at the bottom of the record producer form.

**Role required:** admin

The base system **Create New Incident** record producer is configured to use contextual search. If you have customized this record producer, you can configure contextual search to link to a specific field on your record producer.

**Note:** Only one variable within a record producer can use contextual search.

1. Navigate to **Contextual Search > Record Producer Configuration** and click **New**.
2. In the form, fill in the fields.

![Record Producer Configuration Form](image)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record producer</td>
<td>Unique name of the record producer where you want to add the contextual search.</td>
</tr>
<tr>
<td>Search context</td>
<td>Name of the search context to use.</td>
</tr>
<tr>
<td>Search variable</td>
<td>Variable within the selected record producer that uses the contextual search.</td>
</tr>
<tr>
<td>Results header text</td>
<td>Unique name that appears as a header for the search results area that appears in the form.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box to activate the record producer configuration.</td>
</tr>
<tr>
<td>Limit</td>
<td>Maximum number of search results returned.</td>
</tr>
<tr>
<td>Results per page</td>
<td>Number of results to display per page.</td>
</tr>
<tr>
<td>Allow expand/collapse</td>
<td>Check box to expand or collapse the search results in the form.</td>
</tr>
</tbody>
</table>

3. Click **Submit**.
Define email configuration for contextual search

Define email configurations to allow the system to include search results with an email notifications.

Role required: admin

When knowledge articles are associated with a record, those search results can be included in email notifications. For example, email notifications sent when an incident is created can include knowledge search results. An article in the search results may help the user, who raised the incident, to resolve the issue independently.

1. Navigate to **Contextual Search > Table Configuration**.
2. In the Email Configurations related list, click **New**.
3. In the form, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email notification</td>
<td>Lookup icon to select an email notification to attach the search results. You can select only from the notifications that are on the same table as the table configuration record.</td>
</tr>
<tr>
<td>User field</td>
<td>A reference field that helps to narrow down on the search results. For example, if you select <strong>Opened by</strong>, the search results include only the articles that the <strong>Opened by</strong> user can access based on user criteria.</td>
</tr>
<tr>
<td>Application</td>
<td>Application scope of the email configuration. The configuration is available for all applications or for scoped applications.</td>
</tr>
<tr>
<td>Limit</td>
<td>Maximum number of search results returned.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

Provide knowledge in incident email notification

Contextual search results are included in email notifications that are sent to users who create a new incident.

Role required: admin

The email notification provides links to knowledge articles that may help users resolve their issues faster. For example, if a user raises an incident when the service desk staff is not available, the email notification provides knowledge links that may help the user.

By default, contextual search results are based on the short description in the incident. Within the automated email response, contextual search adds links to relevant knowledge articles.

1. A customer sends an email to IT support with the subject **My laptop keeps crashing**.
2. An incident is created based on this email.
3. The email subject is inserted into the **Short description** field of the new incident.
4. The automated email notification sent to the user includes search results based on **My laptop keeps crashing**.

By default, notifications provide three article links.
5. The customer may then be able to use the search results to resolve the incident.

**Note:** The knowledge links provided are filtered to ensure that the articles are accessible to the user who submitted the email.

You can configure notification options, such as changing the number of links provided with notifications. You can also configure contextual search functionality to match the email notifications of your organization or you can use contextual search with notifications for other records.

**Edit an email notification for the search results**

Edit the email notification that is sent to include search results.

Role required: admin

1. Navigate to **System Notification > Email > Notifications**.
2. Open the email template that you want to edit.
3. Click **What it will contain**.
4. In the **Message HTML** field, add the following script:

   `_${mail_script.cxs_EmailSearchResults}_`

5. Right-click on the header form and click **Save**.
Attach a knowledge article

Attach a knowledge article to an incident to solve issues quickly by going through the in-depth troubleshooting steps and other detailed information in the article.

1. Navigate to Incident > All.
2. Open an active incident record.

In the Related Search Results, search results appear.
3. Click **Attach** for the knowledge article that you want to attach with the incident record. A note about the knowledge article is copied or appended to the **Additional comments (Customer visible)** field. If you want to change the field, refer to **Specify field for attached knowledge article links**.

4. Click **Post** or right-click the header of the form and click **Save** to add the note to the activity stream.

**Specify field for attached knowledge article links**

Specify which field to add a note to when you attach a knowledge article to a record. By default, a link of the knowledge article is added to the **Additional comments (Customer visible)** field. You can specify the field based on the table. For example, a Problem record does not have **Additional comments (Customer visible)** field on the form. The **Attach** action is configured to add the note to the **Work notes** field.

Role required: admin

You can specify the field either globally or locally. The local field for a table overrides the global default field value.

To specify the global field, navigate to **Knowledge > Administration > Properties > Other Knowledge Properties** and specify the name of the field in the **glide.knowman.attach.fields** property.

You can specify the local field using the following procedure.

1. Navigate to **Contextual Search > Table Configuration**.
2. Edit the table configuration that you want to change attachment fields for.
3. Click the Search Action Configurations related list.
4. For each search action that you want to change the default field for, perform the following steps:
   a) Edit the search action.
   b) Select the **Use custom field for attach note** option, if not already selected.
   c) In the **Attach note field**, enter the name of the field that you want the copy the article into, such as `comments` or `work_notes`.
   d) Click **Update**.

**Note:**
- If you do not want to add a note to any field, leave the **Attach note field** blank.
- If the field you have specified in the **Attach note field** is not found on the form, then the note is not added to any field.

Clear the system cache to make sure the changed field specification applies. You can clear the system cache by appending `cache.do` to the instance URL. For example, `https://<instance name>.service-now.com/cache.do`.

**Warning:**
Clearing the system cache can affect overall performance and degrade system response times. Do not run cache flushes during business hours, and do not trigger cache flushes automatically.

**Feedback information on contextual search**

When a user clicks any of the action buttons such as **This helped**, **Order**, or **Attached**, the feedback information is stored in specific tables. The information helps you to understand the effectiveness of the searches. You can also create custom reports by querying these tables.

<table>
<thead>
<tr>
<th>Table [name]</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relevant Document Detail [cxs_rel_doc_detail]</td>
<td>The list of individual recorded actions. For example, Preview, This helped, Attach, or Order. The key fields in the Relevant Document Detail table are as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Original search terms</strong>: The original search terms. This field is used only when the fulfiller has overridden the original search terms using the related search box.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Relevance type</strong>: The recorded action.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Relevant document</strong>: The reference to the search session group in the Relevant Document table.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Created by</strong>: The user who performed the action.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Position</strong>: The position of the recorded action in the result list.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Search Resource</strong>: The reference to the search resource for that particular result. Used only for an Predictive Intelligence Similarity result.</td>
</tr>
</tbody>
</table>
Run a report on contextual search usage

Run a report on usage such as how many times a knowledge article is attached to a record to know the effectiveness of the contextual search results.

Role required: admin

A service desk manager can generate a report on user issues that were resolved without an incident being raised. The information can help to create targeted knowledge based on trends. You can analyze commonly raised incidents and then create knowledge articles around those incidents which can help resolve or deflect similar incidents in future.

1. Navigate to Reports > View/Run.
2. Click Create a report.
3. Under Data, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report name</td>
<td>Unique name for the report.</td>
</tr>
<tr>
<td>Source type</td>
<td>Source from which the data is populated. The default value is Table.</td>
</tr>
<tr>
<td>Table</td>
<td>Select the Relevant Document Detail table [cxs_rel_doc_detail].</td>
</tr>
</tbody>
</table>

4. Under Type, click Next.
5. Under Configure, click Next.
6. Click **Choose columns** and move the required fields from the **Available** box to the **Selected** box.
7. Click **OK** and then click **Run**.
<table>
<thead>
<tr>
<th>Created</th>
<th>Created by</th>
<th>Search term</th>
<th>Original search terms</th>
<th>Relevance type</th>
<th>Position</th>
<th>Relevant doc title</th>
<th>Relevant document</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>2023-05-31</td>
<td>admin</td>
<td>email</td>
<td></td>
<td>This helped</td>
<td>-</td>
<td>Knowledge (knowledge)</td>
<td></td>
<td>empty</td>
</tr>
<tr>
<td>2023-05-31</td>
<td>admin</td>
<td>Please remove the latest UAT's from my PC</td>
<td></td>
<td>This helped</td>
<td>-</td>
<td>Knowledge (knowledge)</td>
<td></td>
<td>empty</td>
</tr>
<tr>
<td>2023-05-17</td>
<td>admin</td>
<td>Need to remove used functionality</td>
<td></td>
<td>search</td>
<td>-</td>
<td>-</td>
<td></td>
<td>empty</td>
</tr>
<tr>
<td>2023-05-15</td>
<td>admin</td>
<td>SAP landscape</td>
<td></td>
<td>search</td>
<td>-</td>
<td>Knowledge (knowledge)</td>
<td></td>
<td>empty</td>
</tr>
<tr>
<td>2023-05-14</td>
<td>admin</td>
<td>SAP sales</td>
<td></td>
<td>search</td>
<td>-</td>
<td>Knowledge (knowledge)</td>
<td></td>
<td>empty</td>
</tr>
<tr>
<td>2023-05-13</td>
<td>admin</td>
<td>SAP landscape</td>
<td></td>
<td>search</td>
<td>-</td>
<td>Knowledge (knowledge)</td>
<td></td>
<td>empty</td>
</tr>
<tr>
<td>2023-05-12</td>
<td>admin</td>
<td>SAP sales</td>
<td></td>
<td>search</td>
<td>-</td>
<td>Knowledge (knowledge)</td>
<td></td>
<td>empty</td>
</tr>
<tr>
<td>2023-05-11</td>
<td>admin</td>
<td>Please remove the latest UAT's from my PC</td>
<td></td>
<td>This helped</td>
<td>-</td>
<td>Knowledge (knowledge)</td>
<td></td>
<td>empty</td>
</tr>
<tr>
<td>2023-05-11</td>
<td>admin</td>
<td>SAP landscape</td>
<td></td>
<td>search</td>
<td>-</td>
<td>Knowledge (knowledge)</td>
<td></td>
<td>empty</td>
</tr>
<tr>
<td>2023-05-11</td>
<td>admin</td>
<td>SAP landscape</td>
<td></td>
<td>search</td>
<td>-</td>
<td>Knowledge (knowledge)</td>
<td></td>
<td>empty</td>
</tr>
<tr>
<td>2023-05-11</td>
<td>admin</td>
<td>SAP landscape</td>
<td></td>
<td>search</td>
<td>-</td>
<td>Knowledge (knowledge)</td>
<td></td>
<td>empty</td>
</tr>
<tr>
<td>2023-05-11</td>
<td>admin</td>
<td>Microsoft</td>
<td></td>
<td>search</td>
<td>-</td>
<td>Knowledge (knowledge)</td>
<td></td>
<td>empty</td>
</tr>
<tr>
<td>2023-05-11</td>
<td>admin</td>
<td>CRM function</td>
<td></td>
<td>search</td>
<td>-</td>
<td>Knowledge (knowledge)</td>
<td></td>
<td>empty</td>
</tr>
<tr>
<td>2023-05-11</td>
<td>admin</td>
<td>SAP landscape</td>
<td></td>
<td>search</td>
<td>-</td>
<td>Knowledge (knowledge)</td>
<td></td>
<td>empty</td>
</tr>
</tbody>
</table>
**Note:** When users select the **Search on tab** check box in Table Configuration and then modify and leave the search field, an action gets logged in the Relevant Document Detail table [cxs_rel_doc_detail]. The information in the table can help you find the instances where users ran a search but did not take any action. In those cases, the value of the **Position** column is `-1`.

---

**Domain separation and Contextual Search**

Domain separation is supported in Contextual Search. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can control several aspects of this separation, including which users can see and access data.

**Support level: Standard**

- Includes **Basic** level support.
- Business logic: The service provider (SP) creates or modifies processes per customer. The use cases reflect proper use of the application by multiple SP customers in a single instance.
- The instance owner must configure the minimum viable product (MVP) business logic and data parameters per tenant as expected for the specific application.

Use case: An admin must be able to make comments required when a record closes for one tenant, but not for another.

To learn more, see Application support for domain separation.

**How domain separation works in Contextual Search**

By default, Contextual Search Suggestions results that appear use the domain of the currently logged-in user.

**Search as a different user**

In addition to being able to search for results using the domain of the logged-in user, the administrator can also configure Contextual Search to **Search as a different user**.

When **Search as** is configured, two tabs appear in the search results:

1. **My Results** tab searches using the currently logged-in user domain.
2. The **Search as** user tab searches using the domain of the User Reference field selected by the administrator. For example: The domain of the user who made the request (**Opened by** or **Caller** fields).

**Note:**

- The search as user results apply security access to display results that are common to both the logged in user and the search as user. Hence, the search result view for that user may have fewer entries than what that user can actually view.
- Record producers only support searching as the currently logged in user.

Example: The Incident's short description displaying My Results (the currently logged-in user).
Example: The Incident's short description displaying the caller results (reference field).
CMDB Search

Query on CMDB CIs and relationships by entering a search text with configurable synonyms and stop words, which CMDB Search converts into a properly formulated query.

CMDB Search is integrated into global text search, providing enhanced capabilities for searching the CMDB. CMDB Search is designed to search within CMDB tables and relationships, allowing for queries that are more complex than basic text search. For example, you can query for all Tomcat instances that are running on Linux, or for all applications of a specific version that are running on Linux.

CMDB Search parses the search text that you enter, to formulate a properly formatted query that runs on the CMDB. Your search text can include plain words which are then parsed to identify any CMDB table, column, or relationship names. CMDB Search also uses synonyms and stop words to replace any plain text strings within your search text.
Localization is not supported for CMDB Search. In a localized instance, query words such as CI, relationship, or server, must be in English.

**Stop Words**

A collection of words that are ignored when CMDB Search parses your search text. When CMDB Search finds a stop word in your search text, that word is ignored. CMDB Search provides default stop words such as 'if', 'me', and 'have'. You can delete or add stop words.

To view stop words, navigate to Configuration > CMDB Search > Stop Words.

**Relation Synonyms**

A collection of synonyms for relationships. CMDB Search searches your search text for strings that match any relationship synonym. For any such string that is found, CMDB Search replaces that string with the relationship type specified in the relation synonym. CMDB Search provides relationship synonyms for common words that stand for any relationship between two tables. For example, the strings "connect", "in", and "on" in your search text, are all treated as a general reference to a relationship, without specifying any relationship in particular. You can modify, delete, or add relationship synonyms.

To view relationship synonyms, navigate to Configuration > CMDB Search > Relation Synonyms.

**CI Class Synonyms**

A collection of synonyms for CI classes. CMDB Search searches your search text for strings that match any CI class synonym. For any such string that is found, CMDB Search replaces that string with the CI class name specified in the CI class synonym. CMDB Search provides at least one default CI class synonym for each CMDB table. Most default CI class synonyms are the class label. You can modify, delete, or add CI class synonyms.

To view CI class synonyms, navigate to Configuration > CMDB Search > CI Class Synonyms.

**Column Synonyms**

A collection of synonyms for table columns. CMDB Search searches your search text for strings that match any column synonym. For any such string that is found, CMDB Search replaces that string with the column name specified in the column synonym. CMDB Search provides at least one default column synonym for each table column in the CMDB. Most default column synonyms are similar to the column name itself. You can modify, delete, or add column synonyms.

To view column synonyms, navigate to Configuration > CMDB Search > Column Synonyms.

CMDB Search supports domain separation, searching CIs according to the user domain.

**Plugin**

To use CMDB Search, activate the CMDB Search (com.snc.cmdb_search) plugin. Activating CMDB Search triggers Zing text search indexing of all CMDB tables, since the Zing search engine is required for some CMDB Searches.

**Search text format and examples**

The format of the search text is:

```
(<CI class name> (<attribute> "value")* (<relationship>))*)
```

Consisting of a table name, followed by pairs of `<column> "<value>">`, without any separating commas, and with values surrounded by quotation marks. For column, table, and relationship names, you can search by actual names, labels, or synonyms, and column names can be omitted.

Examples:

- application runs on ci name "ciname"
• application name "JBoss Server13" version "1.0.0.0" on tomcat name "Tomcat10" version "2.1"
• tomcat on linux
• tomcat name “My Tomcat” version “2.0” running on linux server name “Linux8”
• tomcat “My Tomcat”
• tomcat name “My Tomcat”
• tomcat name related to Linux server “my server”
• tomcat name related to Linux server ip 1.1.1.1
• services related to tomcat “my tomcat”
• CI impacted by service “EmailService”

Sometimes the search text contains a name, such as Port, which is both a class and a column name. In this situation, the CMDB Search strategy is to first search for a class with the specified name, and then search for a column with the specified name. If this strategy does not yield the expected results, then use the actual class or column name to prevent ambiguity.

**Results**

Up to 10 query results appear after running the query. To view any additional results, click **View all <record> matches**. The total number of results that you can view depends on the value of the `cmdb.search.rows.limit` system property, which is set to 100 by default. You can increase this property value, or you can change the query to return a smaller number of results. Increasing the number of query results might impact performance.

**Events**

Events are special records the system uses to log when certain conditions occur and to take some kind of action in response to the conditions.

The system uses business rules to monitor for system conditions and to generate event records in the Event [sysevent] table, which is also known as the event log or event queue.

Event-generating business rules typically use this script logic:

If [some condition is true for the current record], then [add a specific event to the queue].

For example, here are some of the conditions in the **incident event** business rule:

• If a user adds a comment to an incident record, add an **incident.commented** event.
• If a user adds an incident record, add an **incident.inserted** event.
• If a user updates an incident record, add an **incident.updated** event.

Event-generating business rules use the GlideSystem `eventQueue` method to insert event records, which typically contain this information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name of event. Baseline event names include the record affected and the triggering action, such as <strong>incident.commented</strong>.</td>
</tr>
<tr>
<td>Parm1</td>
<td>Event-specific parameter the system uses to pass record information to other parts of the system, such as a record Sys ID or a field value.</td>
</tr>
</tbody>
</table>
Scheduled jobs periodically read the event queue and forward them to the appropriate handler for processing. The handler uses information from event records to take some kind of action such as:

- Run a script action
- Schedule a job
- Send a notification
- Trigger a workflow activity
- Trigger an inactivity monitor

By default, the system provides events covering a broad view of application activity. If existing events do not meet your needs, you can create your own events to watch for specific changes to records.

For developer training, see Scheduled Script Executions and Events Objectives on the ServiceNow® Developer Site.

### Event registry

The events registry lists the events the system recognizes. Use registered events to automate other activities, such as script actions or notifications.

After you create a new event and a business rule that uses the event, you must register it.

Registration lets other parts of the system, such as Email Notifications and Script Actions, see the event in their list of available events and react to the event when it occurs.

### Event states

The event state describes where in the life cycle the event is.

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ready</td>
<td>The system created the event and it is in the queue waiting to be processed.</td>
</tr>
<tr>
<td>Processed</td>
<td>The event successfully ran. An event does not necessarily trigger any further action when processed. Additional functionality must make use of the event.</td>
</tr>
<tr>
<td>Error</td>
<td>The event encountered an error during processing. This state is often caused by invalid event parameters. Reprocessing the event may resolve the error.</td>
</tr>
</tbody>
</table>
### Event logs

The event log records all system events that occur within the Now Platform.

This log provides the following information for all events that occur:

#### Event log

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created</td>
<td>Date and time of the event for the locale of the machine running the instance.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the event as listed in the Event Registry.</td>
</tr>
<tr>
<td>URI</td>
<td>HTTP query that generated the event.</td>
</tr>
<tr>
<td>Parm1</td>
<td>Event-specific value that depends on the event and the recipient.</td>
</tr>
<tr>
<td>Parm2</td>
<td>Event-specific value that depends on the event and the recipient.</td>
</tr>
<tr>
<td>Table</td>
<td>Database table acted on for this event.</td>
</tr>
<tr>
<td>Processed</td>
<td>Date and time the event was processed This time reflects the locale of the machine running the instance.</td>
</tr>
<tr>
<td>Processing time</td>
<td>Time taken to process this event, in milliseconds.</td>
</tr>
<tr>
<td>Queue</td>
<td>Processor queue name.</td>
</tr>
</tbody>
</table>
The incident events business rule

The incident events business rule comes with the system and defines a number of events that can be triggered by different actions in the Incident table.

Incident events business rule

This business rule defines several events, three of which are triggered after a record in the Incident table is inserted or updated. The first script is:

```java
if (current.operation() != 'insert' && current.comments.changes()) {
    gs.eventQueue("incident.commented", current, gs.getUserID(), gs.getUserName());
}
```

The condition in this script requires that a change be made to the Comments field in an existing (not inserted) incident record. If this condition is true, then the platform adds the incident.commented event to the event queue.
The second condition requires that a record be inserted before the event is added to the queue.

```java
if (current.operation() == 'insert') {
    // Code here
}
```

The third condition is true whenever the incident record is updated (including updates to the **Comments** field, as specified by the first script).

```java
if (current.operation() == 'update') {
    // Code here
}
```

The then part of each script, the `gs.eventQueue` function, adds the event to the event queue. This statement uses the following syntax, set off with braces:

```java
gs.eventQueue("incident.updated", current, gs.getUserID(),
             gs.getUserName());
```

The `gs.eventQueue` function takes the following parameters:

<table>
<thead>
<tr>
<th>Field</th>
<th>Input Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the event triggered, set in quotation marks</td>
</tr>
<tr>
<td>Record</td>
<td>The record referenced when the condition in the script evaluates to <code>true</code>. Usually this is expressed as <code>current</code>, meaning the current record the business rule is working on. If the business rule is being triggered as part of a scheduled job, use a GlideRecord argument in its place.</td>
</tr>
<tr>
<td>Parm 1</td>
<td>An optional parameter you can use to pass system or record information with the event. For example, the GlideSystem API call <code>gs.getUserID()</code> passes the Sys ID of the user who acted on the current record as a string value. Other scripts can reference this string value as <code>parm1</code> using the format <code>${event.parm1}</code>.</td>
</tr>
<tr>
<td>Parm 2</td>
<td>An optional parameter you can use to pass system or record information with the event. For example, the GlideSystem API call <code>gs.getUserName()</code> passes the user name of the user who acted on the current record. Other scripts can reference this string values as <code>parm2</code> using the format <code>${event.parm2}</code>.</td>
</tr>
</tbody>
</table>

**Note:** The `gs.EventQueue` function works directly with the backend and therefore business rules that are called by `gs.EventQueue()` are not invoked.

### Sample scripts from the change events business rule

Several scripts are found in the baseline change events business rule.

This business rule defines events that fire after a change request is inserted or updated.

```java
if (current.operation() == 'insert') {
    gs.eventQueue("change.inserted", current, gs.getUserID(),
                 gs.getUserName());
}
```

```java
if (current.operation() == 'update') {
    gs.eventQueue("change.updated", current, gs.getUserID(), gs.getUserName());
}
```
if (!current.assigned_to.nil() && current.assigned_to.changes()) {
    gs.eventQueue("change.assigned", current,
    current.assigned_to.getDisplayValue(),
    previous.assigned_to.getDisplayValue());
}

if (current.priority.changes() && current.priority == 1) {
    gs.eventQueue("change.priority.1", current, current.priority,
    previous.priority);
}

if (current.risk.changes() && current.risk == 1) {
    gs.eventQueue("change.risk.1", current, current.risk, previous.risk);
}

if (current.start_date.changes() || current.end_date.changes() ||
    current.assigned_to.changes()) {
    if (!current.start_date.nil() && !current.end_date.nil() && !
    current.assigned_to.nil()) {
        gs.eventQueue("change.calendar.notify", current, current.assigned_to,
        previous.assigned_to);
    }
}

// Remove from previous assigned to, due to assigned_to changing
if (!previous.assigned_to.nil()) {
    if (!previous.assigned_to.nil() && current.assigned_to.changes() &&
        !previous.start_date.nil() && !previous.end_date.nil()) {
        gs.eventQueue("change.calendar.notify.remove", current,
        current.assigned_to, previous.assigned_to);
    }
}

// Remove old calendar from current assigned to, due to date changing
else if (!current.assigned_to.nil()) {
    if ((current.start_date.changes() && !previous.start_date.nil()) ||
        (current.end_date.changes() && !previous.end_date.nil())) {
        gs.eventQueue("change.calendar.notify.remove", current,
        current.assigned_to, "current.assigned_to");
    }
}


Script actions

You can use script actions to create server-side scripts that perform a variety of tasks, such as modifying a
collection item (CI), or managing failed login attempts. Script actions are triggered by events only.

Configuration

To create a new script action, navigate to System Policy > Events > Script Actions and click New.

<table>
<thead>
<tr>
<th>Field</th>
<th>Input Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a unique name for your script action.</td>
</tr>
<tr>
<td>Event Name</td>
<td>Select the event to use for this script. If you do not find an event for your script action that suits your purpose, you can create a new one.</td>
</tr>
<tr>
<td>Field</td>
<td>Input Value</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Application</td>
<td>The application that contains this script.</td>
</tr>
<tr>
<td>Order</td>
<td>The order in which the script will be executed.</td>
</tr>
<tr>
<td>Active</td>
<td>Select the check box (true) to enable this script action.</td>
</tr>
<tr>
<td>Condition Script</td>
<td>Create a statement for a condition under which this script should execute. The system only parses the <strong>Script</strong> field if the condition evaluates to true. If you decide to include the condition statement in the script, leave this field blank.</td>
</tr>
<tr>
<td>Script</td>
<td>Create a script that runs when the condition you define evaluates to true. Two additional objects are available in this script: [ \begin{itemize} \item event: a GlideRecord - the sysevent that caused this to be invoked. If you wanted so get this first parameter on the event, you would use event.parm1 or event.parm2 for the second parameter. For the date/time of the event, use event.sys_created_on. To get the user ID that created the event (if there was a user associated), use event.user_id. \item current: a GlideRecord - the event scheduled on behalf of (incident for example). \end{itemize} ]</td>
</tr>
</tbody>
</table>

This is a sample of a script action that creates an email notification for Workflow activity:
```javascript
function sendWorkflowNotification() {
  // get the activity that defines the information about the event
  var activity = new GlideRecord('wf_activity');
  if (activity.get(parts)) return 0;

  // The EmailAction does not know how to handle \${workflow...} constructs so we need to handle those for it
  var context = new GlideRecord('wf_context');
  if (parts.length == 1) context.put(parts[0]);

  GlideController.putGlobal('context', context);
  var workflow = new Workflow(workflow, new WorkflowProxy());
  GlideController.putGlobal('workflow', workflow);

  var subject = new GlideEmailAction('subject', workflowactivity vars subject);
  var email = new GlideEmailAction('email', workflowactivity vars email);
  var email = new GlideEmailAction('email', workflowactivity vars email);
  var email = new GlideEmailAction('email', workflowactivity vars email);
  var email = new GlideEmailAction('email', workflowactivity vars email);
```
Global events

Your instance has a global function called `global_events()` that triggers from a business rule when certain conditions occur.

This function triggers when your instance is:

- Inserting new records
- Updating existing records
- Adding comments to an existing record
- Assigning a record to a user
- Exceeding a record's inactive timer

For example, if you add the script `global.events(current)` to a business rule on the `change_request` table, the instance automatically configures the following events:

- `change_request.inserted`
- `change_request.updated`
- `change_request.commented`
- `change_request.assigned`
- `change_request.inactive`

The business rule for global events on the `change_request` table looks like this:

![Business Rule](image)

Change request tasks global business rule
Create an event

If you do not find a suitable existing event, you can create your own.

Role required: admin

The gs.EventQueue function works directly with the backend and therefore business rules that are called by gs.EventQueue() are not invoked.

1. Navigate to System Policy > Events > Registry.
2. Click New and fill in the form.
3. Click the Business Rules related link.
4. If you are creating an event for a base system table, select the existing event business rule for the table. For example, select the sc request events business rule to create a custom Request event.
5. If you are updating an existing event business rule, add a new condition to the Script. The following sample script adds a request commented event with the user's Sys ID as parm1 and the user's user name for parm2.

   ```javascript
   if (current.operation() != 'insert' && current.comments.changes()) {
     gs.eventQueue('request.commented', current, gs.getUserID(),
     gs.getUserName());
   }
   ```

6. If you are creating an event for a custom table, create a new business rule that runs after database operations. For example, this business rule defines several events for a custom application called Marketing Events.

   **Sample event business rule**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Attendee Events</td>
</tr>
<tr>
<td>Table</td>
<td>Attendee [x_snc_marketing_ev_attendee]</td>
</tr>
<tr>
<td>Application</td>
<td>Marketing Events</td>
</tr>
<tr>
<td>Advanced</td>
<td>Selected</td>
</tr>
<tr>
<td>When</td>
<td>after</td>
</tr>
<tr>
<td>Insert</td>
<td>Selected</td>
</tr>
<tr>
<td>Update</td>
<td>Selected</td>
</tr>
<tr>
<td>Delete</td>
<td>Selected</td>
</tr>
<tr>
<td>Script</td>
<td>Add custom script that:</td>
</tr>
<tr>
<td></td>
<td>• Checks for one or more conditions on the current record.</td>
</tr>
<tr>
<td></td>
<td>• Calls the gs.eventQueue() method and specifies an event name.</td>
</tr>
<tr>
<td></td>
<td>See code sample.</td>
</tr>
</tbody>
</table>

**Note:** If you add Filter Conditions, Role conditions, or a Condition value, verify it runs the business rule when expected.
//This function will be automatically called when this rule is processed.
//Add event when attendee inserted
if (current.operation() == 'insert' &&
current.marketing_event.changes()) {
  gs.eventQueue('x_snc_marketing_ev.attendee.added',
  current,
  current.marketing_event, current.email);
}
//Add event when marketing event changes
if (current.operation() == 'update' &&
current.marketing_event.changes()) {
  gs.eventQueue('x_snc_marketing_ev.attendee.deleted',
  previous,
  previous.marketing_event, previous.email);
  gs.eventQueue('x_snc_marketing_ev.attendee.added',
  current,
  current.marketing_event, current.email);
}
//Add event when attendee deleted
if (current.operation() == 'delete') {
  gs.eventQueue('x_snc_marketing_ev.attendee.deleted',
  current,
  current.marketing_event, current.email);
}
})(current, previous);

7. Register the event.

Create a script action or notification to process the event.

Register an event

You can register an event for a specific table and a business rule that fires the event.

1. To register an event, browse to System Policy > Events > Registry, and then click New.
2. On the form fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of your new event.</td>
</tr>
<tr>
<td>Table</td>
<td>Database table for this event.</td>
</tr>
<tr>
<td>Description</td>
<td>Short description of the purpose of the event.</td>
</tr>
<tr>
<td>Fired by</td>
<td>Name of the business rule that runs the event. This field is for reference only and is not used by any process. Make sure that there is enough information to locate your event again.</td>
</tr>
<tr>
<td>Queue</td>
<td>Name of the queue that the event is placed into when triggered.</td>
</tr>
</tbody>
</table>

Note: Only tables and database views that are in the same scope as the event appear on the listing.
Reprocess an event

You can fire the event again for testing or diagnostic purposes.

Role required: admin

1. Navigate to System Logs > Events.
2. Open an event.
   The event returns to the event queue.

Pass event parameters from a workflow to a notification

You can pass two event parameters that send information about a record or related records from a workflow to a notification.

Role required: admin

1. Navigate to System Policy > Events > Registry and define a new event to call.
2. Create the activity step that calls the event from your workflow and assign the two possible parameters.
   These parameters can be references or fields on the record that triggered the workflow, such as current.number for the request item number. You can also dot-walk to records in other tables. The event then sends the parameters information to the notification that it triggers.
3. Retrieve the parameters in the notification with email scripts by using event.parm1 and event.parm2.
   For example:

   ```javascript
   var string = event.parm1.toString();
   template.print(string);
   ```

   Another example using Sys IDs gives you access to anything in the record that triggered the workflow. Use a script like this to send information about a change or request to support personnel, for example.

   ```javascript
   var id = event.parm1.toString();
   var now_GR = new GlideRecord('sc_req_item');
   gr.get('sys_id', id);
   if (gr.next()){
     // Do something.
   }
   ```

Data management

Data is stored and managed in your instance according to a principled structure that administrators can view and configure. Data management functions include importing, exporting, and archiving database data and configuring fields and tables.

Database structure

All of the information in the instances is stored in tables, which consist of a series of records. The record in turn holds a series of fields that hold the individual bits of data and can be viewed either as a list or a form.
Tables can be related to each other in the following ways:

**Extensions**

A table can extend another table. The table doing the extending (child class) includes all of the fields of the other table (parent class) and adds its own fields. For instance, the Incident [incident] table has all of the Task [task] table fields (because an incident is a special form of task) and has its own incident-specific tasks.

**One-to-Many**

Within a table, a field can hold a reference to a record on another table. There are three types of one-to-many relationship fields:

- **Reference Field**: allow a user to select a record on a table defined by the reference field. For instance, the **Caller** field on the Incident table allows the user to select any record on the User table.
- **Glide List**: allows a user to select multiple records on a table defined by the glide list. For instance, the **Watch list** field on the Incident table allows the user to select records on the User table.
- **Document ID Field**: allows a user to select a record on any table in the instance. These fields are much less common, but one example is the **Document** field on the Translated Text [sys_translated_text] table.

**Many-to-Many**

Two tables can have a bi-directional relationship, so that the related records are visible from both tables in a related list.

**Database Views**

Two tables can be joined virtually with Database Views to enable reporting on data that might be stored over more than one table.

**Data management tools**

There are a number of tools that can help manage data within the instance.

**Schema map**

The Schema Map displays the relationships between tables visually, helping to navigate through the database structure.

The Schema Map provides an interface for viewing the relationships between tables. The inter-table relationships it captures include many-to-many relationships, tables that extend other tables, and tables that reference other tables through reference fields.

**Data dictionary tables**

Data dictionary tables holds information that defines the database and can be accessed for information on the database schema.

These tables hold important information on the database and its structure:

- **Tables [sys_db_object]**: contains a record for each table.
- **Dictionary Entries [sys_dictionary]**: contains additional details for each table and the definition for every column on each table. Each row represents either a column on a table or a table.
- **Field Labels [sys_documentation]**: contains the human-readable labels and language information.

**Table cleaner**

Table cleaner automatically deletes records on certain tables to prevent data growing exponentially. Records are automatically deleted from specific tables after a specific time to deletion. Deleting these records automatically prevents the tables from growing to an unmanageable size.
The time before a record is deleted begins on the date and time value in the tracked field. The Table Cleaner scheduled job runs the table cleaner every hour. To view the list of tables that are auto-cleaned, in the Navigator filter, type: sys_auto_flush_list.do. All records with \[\text{MatchField} < (\text{current_time} - \text{Age in seconds})\] are deleted.

- The \text{MatchField} field represents a Date/Time column in the table that you are trying to clean up.
- The \text{Age in seconds} field represents a value in seconds.

You can set up multiple table cleaner entries for a particular table. Performance depends on the size of the table and the conditions used. For example, if you use a custom column in a very large table that has no index on, performance is severely degraded. Performance also depends on the number of rows to be deleted.

\[\text{Note: TableCleaner does not call DBDelete.setWorkflow()}. \text{This means DBDelete objects run with workflow=false (false is the default value for a Java boolean), hence Delete business rules and workflows are not triggered.}\]

### Cleaned tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Tracked field</th>
<th>Time to deletion</th>
</tr>
</thead>
<tbody>
<tr>
<td>sys_poll</td>
<td>sys_created_on</td>
<td>1 day</td>
</tr>
<tr>
<td>cmdb_metric</td>
<td>sys_created_on</td>
<td>2 days</td>
</tr>
<tr>
<td>ecc_agent_metric</td>
<td>sys_created_on</td>
<td>30 days</td>
</tr>
<tr>
<td>v_transaction</td>
<td>sys_created_on</td>
<td>1 day</td>
</tr>
<tr>
<td>wf_context</td>
<td>ended</td>
<td>180 days</td>
</tr>
<tr>
<td>sys_cache_flush</td>
<td>sys_created_on</td>
<td>1 hour</td>
</tr>
<tr>
<td>sys_replication_queue</td>
<td>sys_created_on</td>
<td>1 day</td>
</tr>
<tr>
<td>sysevent</td>
<td>sys_created_on</td>
<td>7 days</td>
</tr>
<tr>
<td>ecc_queue</td>
<td>sys_created_on</td>
<td>30 days</td>
</tr>
<tr>
<td>syslog</td>
<td>sys_created_on</td>
<td>90 days</td>
</tr>
<tr>
<td>sys_querystat</td>
<td>sys_created_on</td>
<td>30 days</td>
</tr>
<tr>
<td>plan_execution</td>
<td>sys_created_on</td>
<td>30 days</td>
</tr>
<tr>
<td>sys_user_session</td>
<td>last_accessed</td>
<td>1 day</td>
</tr>
<tr>
<td>sys_user_preference</td>
<td>sys_updated_on</td>
<td>1 day</td>
</tr>
<tr>
<td>sys_history_set</td>
<td>sys_updated_on</td>
<td>30 days</td>
</tr>
<tr>
<td>label_history</td>
<td>sys_created_on</td>
<td>30 days</td>
</tr>
<tr>
<td>ts_search_summary</td>
<td>sys_created_on</td>
<td>30 days</td>
</tr>
<tr>
<td>sys_cluster_message</td>
<td>sys_created_on</td>
<td>1 day</td>
</tr>
<tr>
<td>cmdb_tcp_connection</td>
<td>sys_updated_on</td>
<td>30 days</td>
</tr>
<tr>
<td>cmdb_running_process</td>
<td>sys_updated_on</td>
<td>30 days</td>
</tr>
</tbody>
</table>
## Data management plugins

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Archiving</td>
<td>Provides the ability to archive records to minimize performance issues.</td>
</tr>
<tr>
<td>Database Rotations</td>
<td>Provides tools for managing large tables to minimize performance issues.</td>
</tr>
<tr>
<td>Many to Many task relations</td>
<td>Provides the ability to define many-to-many relationships between task tables.</td>
</tr>
</tbody>
</table>

## Unique record identifier (sys_id)

A unique 32-character GUID (Globally Unique ID), called a Sys ID (sys_id) identifies each record in an instance. There are various ways a record is assigned a sys_id.

When created within the application, sys_id values are unique. The Now Platform and database should manage all operations on sys_id values. The same sys_id value is never generated twice, which ensures that every record created in every table in every instance in the world has a unique identifier. If two records have the same sys_id value, it occurs as a result of the following situations:

- If a record with the sys_id was copied to the other at the database level outside of the Now Platform.
- If a record with the sys_id was copied using an Update Set or via XML, its sys_id is the same.

### Note:

A new record has a sys_id of -1, and once inserted, it is assigned a new sys_id. The sys_id is not meant to show as a field on a form or as a column in a list. To learn more, see the Users are unable to add the sys_id field to a form or list view [KB0690876] article in the Now Support Knowledge Base.

## Get the sys_id from the header bar

Users can locate the sys_id of a record using the header bar.

1. **Navigate to the record.**
2. **Right click the header bar and select Copy URL.**

   The sys_id is inside of the URL, after the parameter sys_id=. For example, the following is a URL for an Incident:

   ```
   https://<instance name>.service-now.com/nav_to.do?uri=incident.do?sys_id=9d385017c611228701d22104cc95c371
   ```

   Therefore the sys_id is 9d385017c611228701d22104cc95c371.

## Get the sys_id from a script

Users can locate the sys_id of a record using a script.

- The sys_id value of a record can be found in a business rule (or any other server-side JavaScript) by dot-walking from the GlideRecord.

   ```
   var id = current.sys_id;
   ```
• The sys_id of a record can be found in client-side JavaScript using g_form.getUniqueValue() as shown in the following example.

```javascript
function onLoad() {
    var incSysid = g_form.getUniqueValue();
    alert(incSysid);
}
```

**Get the sys_id from the URL**

Users can locate the sys_id of a record by viewing the URL.

Since the sys_id of a record is always part of the URL for a link to that record, it is possible to retrieve the sys_id by viewing the URL.

• View the sys_id in the information bar of the browser by hovering over a link to the record.
  
  For example, an Incident with the following URL: https://<instance name>.service-now.com/nav_to.do?uri=incident.do?sys_id=23dc968f0a0a3c1900534f399927740e, has this sys_id: 23dc968f0a0a3c1900534f399927740e.

**Data archiving**

Data archiving involves managing table size growth and archiving old data. It moves data that is no longer needed every day from primary tables to a set of archive tables.

The longer an instance runs, the more likely it is to accumulate data that is no longer relevant. For example, task records from two years ago are typically less relevant than currently active tasks. Old data may eventually cause performance issues by consuming system resources and slowing down queries and reports.

If you cannot delete this data because you need it for auditing or for historical purposes:

1. Set up an archive rule that archives the data and removes it from immediate access to free up system resources.
2. Set up a destroy rule to delete the data after a specified period.
3. Configure the archive and destroy rule properties that control batch processing of the archive and destroy rules.
Sample Benefits of Archiving Data

Data archiving supports Domain separation for service providers. For example, incidents that belong to a domain keep their domain designation even after they are archived.

**Note:** If you want to archive emails, activate the Email retention plugin and use the archive and destruction rules that come with the plugin. Do not use the archive feature to create your own archiving rules on the email table.

Tables and modules created by an archive rule

The first time you activate an archive rule, it performs the following actions:

- Creates the archive table in the database. The archive table has the same name as the primary table with an "ar_" prefix. For example, if you archive the Incident [incident] table, then the archive table is [ar_incident].
• Stores an xml version of each archived record in the sys_archive_log table. This archive log is the same table for all archive rules, and you cannot alter this behavior. It is also the only place where the sys_id is stored together with the display value for reference fields.

For example, for ar_incident \texttt{<assigned_to>Fred Luddy</assigned_to>}, the sys_archive_log record is as follows:

\begin{verbatim}
<assigned_to display_value="Fred Luddy">5137153cc611227c000bbd1bd8cd2005</assigned_to>
\end{verbatim}

• Converts multiple joined tables into a single flat-file archive table. The archive table no longer consists of a base and extended tables.
• Converts reference field values (values set by references to records in other tables) into string values. The archive record contains the display value of the reference field at the time of the archive.
• Adds a module to the Archive Tables list in the System Archiving application. The module name is a combination of the word “Archive” plus the display name for the archived table. For example, the archive module for the Attachment \texttt{[sys_attachments]} table is Archive Attachment. Click the module name to view records in the archive table.
• Creates a list of the archive table using the default list view.
• Creates a form for the archive table using the default form view. The form excludes any dot-walking fields such as Caller ID.Email.
Conversion of Multiple Joined Tables into a Flat Archive Table

Query archived data

Archived tables are not optimized for ad hoc queries. They only contain index entries for the display value, creation date, and the primary key of sys_id.

For this reason, do not make on-demand queries against an archived table, such as searching for all priority 1 archived incidents. Instead, only search against the indexed fields. For example, search for incident INC100001 or incidents created on a specific date.
Archive tables and ACLs

By default, archive tables use the ACLs for the unarchived table of the same name. For example, the archived Incident [ar_incident] table uses the ACLs defined for the unarchived Incident [incident] table.

You can manage access to archive tables explicitly by creating ACLs for specific archive tables and setting the `glide.security.enable_archive_table_acls` property to `true`. The system then follows one of two paths:

1. If one or more active ACLs are defined for an archive table, those ACLs control access to the archive table.
2. If no ACLs are defined for an archive table, the system reverts to default behavior and uses the ACLs for the unarchived version of the table.

**Note:** The two paths are mutually exclusive: If archive table ACLs deny access, the system doesn't attempt to revert to the default behavior.

The read operation read is the only operation evaluated, and other operations are prevented.

The Execution Plan UI is aware of this logic and presents information accordingly. For example, adding the first ACL to an archive table shows that the archive table ACL is "masking" ACLs on the unarchived (original data) table.

If you have existing ACLs on archived tables, they are ignored unless you set the `glide.security.enable_archive_table_acls` property to `true`. Those newly activated ACLs may possibly cause access issues. To prevent this occurrence, the system sets the `glide.security.enable_archive_table_acls` property as follows:

- Instances without the `glide.security.enable_archive_table_acls` property use the default value of `false`.
- Upgraded instances don't install the property. The property must be added manually and set to `true` to enable the archive table ACL behavior.
- Zbooted instances install the property and set it to `true`.

Create an archive rule

The System Archiving application includes several sample archive rules that illustrate the archive features. Related records can be added to an archive rule, and you can view an estimate of the number of records the rule affects.

Role required: admin

The sample archive rules are inactive by default.

**Note:** If you want to archive emails, activate the Email retention plugin and use the archive and destruction rules that come with the plugin. Do not use the archive feature to create your own archiving rules on the email table.

1. Navigate to System Archiving > Archive Rules.
2. Click New.
<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th>Inactive and closed over 9 months</th>
<th><strong>Parent</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Table</strong></td>
<td>Change Request</td>
<td></td>
</tr>
<tr>
<td><strong>Active</strong></td>
<td>False</td>
<td></td>
</tr>
</tbody>
</table>

**Description**
Archive Change Requests (and related change tasks/change phases) that are no longer active and their close date is older than 9 months

**Conditions**

**All of these conditions must be met**

<table>
<thead>
<tr>
<th>Active ▼</th>
<th>is ▼</th>
<th>false ▼</th>
<th>AND ▼</th>
<th>OR ▼</th>
<th>X ▼</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Closed ▼</th>
<th>before ▼</th>
<th>Last 9 months ▼</th>
<th>AND ▼</th>
<th>OR ▼</th>
<th>X ▼</th>
</tr>
</thead>
</table>

**Auto archive**

**Auto archive duration**

<table>
<thead>
<tr>
<th>Days</th>
<th>01</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Hours</th>
<th>00</th>
<th>00</th>
<th>00</th>
</tr>
</thead>
</table>
3. Fill in the fields as appropriate.

**Archive Rule form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Required. Enter a unique name that identifies the rule. Since this name is the display field for archive rules, references to archive rules display the name you enter here.</td>
</tr>
<tr>
<td>Table</td>
<td>Required. Select the table containing records to archive. There can only be one archive rule per table (even if the rule is inactive). If there is an existing archive rule for a table, the table no longer appears as an option on the archive rule table list.</td>
</tr>
<tr>
<td>Active</td>
<td>Select this check box to enable the archive rule. Clear the check box to disable the rule. Leave your archive rules inactive until you calculate an estimate of the number of records the rule affects and verify that rule behaves as expected.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the archive rule.</td>
</tr>
<tr>
<td>Parent</td>
<td>Select an existing archive rule on which this rule depends on to run. This archive rule only runs when the parent rule also runs.</td>
</tr>
<tr>
<td>Conditions</td>
<td>Select the fields and values that must be true in order for the archive rule to run. Typically, you would archive inactive records older than a certain date.</td>
</tr>
<tr>
<td>Auto Rearchive</td>
<td>If a record is restored, this enables the record to be automatically rearchived after a set period of time.</td>
</tr>
<tr>
<td>Auto Rearchive Duration</td>
<td>If you set the Auto Rearchive option, you must set a time interval before the restored record is automatically archived.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

After verifying that the archive rule is selecting records as expected, activate the archive rule.

If you do not want to wait for the scheduled job to run the archive rule, you can manually start the archive rule by clicking **Run Archive Now**.

**Archive related records**

Use the **Archive Related Records** related list to add related records to the archive rule.

Role required: admin

1. Navigate to **System Archiving > Archive Rules**.
2. Select the appropriate archive rule.
3. From the **Archive Related Records** related list, click **New**.
4. Fill in the Archive Related Records form.

**Archive Related Records form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive map</td>
<td>Displays the archive rule to which the related records apply.</td>
</tr>
<tr>
<td>Action</td>
<td>Select the action you want the archive rule to take on related records.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Archive</strong>: archive records that reference the archived record.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Clear</strong>: remove the reference to the archived record. The record no</td>
</tr>
<tr>
<td></td>
<td>longer references the archived record and does not appear as a related</td>
</tr>
<tr>
<td></td>
<td>record in future archives.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Delete</strong>: delete records that reference the archived record.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Reference</td>
<td>Select the relationship of the records you want to apply an action to. The <strong>Reference</strong> field lists all relations that currently exist for the table being referenced. There are two types of possible relations.</td>
</tr>
<tr>
<td></td>
<td>• Another table has a reference field calling the archived table. For example, if you are archiving problem records, there is a <strong>Problem ID</strong> field in the Incident table that references the related problem records.</td>
</tr>
<tr>
<td></td>
<td>• The <strong>Archive</strong> action archives the related record in addition to the primary record. For example, if you select the <strong>Problem in Incident</strong> reference, the related record rule also archives any incident record that references an archived problem.</td>
</tr>
<tr>
<td></td>
<td>• The <strong>Clear</strong> action removes the reference to the primary record. For example, if you select the <strong>Problem in Incident</strong> reference, the related record rule updates any incident record with a reference to the archived problem record by clearing the reference. If the reference is a many-to-many relationship, the related record rule deletes the reference instead of clearing the reference.</td>
</tr>
<tr>
<td></td>
<td>• The <strong>Delete</strong> action deletes any record that references the primary record. For example, if you select the <strong>Problem in Incident</strong> reference, the related record rule deletes any incident record that references the archived problem record.</td>
</tr>
<tr>
<td></td>
<td>• Another table has a <strong>Document ID</strong> field which might point to the archived table. For example, if you are archiving problem records, there is a <strong>sys ID</strong> field in the Attachments table that may reference the problem record. The list indicates document ID relationships by displaying an asterisk (*) character at the end of the selection name.</td>
</tr>
<tr>
<td></td>
<td>• The <strong>Archive</strong> action updates the <strong>Document ID</strong> of the related record to point to the archived table. For example, if you select the <strong>Table sys ID Attachment(sys_attachment)</strong> reference, the related record rule updates the attachment record to change the <strong>Document ID</strong> to refer to the archived table record.</td>
</tr>
<tr>
<td></td>
<td>• The <strong>Clear</strong> action removes the <strong>Document ID</strong> reference to the archived record. The record no longer references the archived record and does not appear as a related record in future archives.</td>
</tr>
<tr>
<td></td>
<td>• The <strong>Delete</strong> action deletes any record that references the primary record. For example, if you select the <strong>Table sys ID Attachment(sys_attachment)</strong> reference, the related record rule deletes any attachment record that references the archived primary.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Reference table</td>
<td>Displays the table where the rule looks for related records.</td>
</tr>
<tr>
<td>Reference element</td>
<td>Displays the reference field or <strong>Document ID</strong> the rule queries for.</td>
</tr>
<tr>
<td>Reference table rule</td>
<td>Select an existing archive rule that applies to the related records you are archiving. For example, if you already have an archive rule for the Incident table, you can select the existing Incident table rule when archiving records related to incidents records.</td>
</tr>
</tbody>
</table>

5. Click **Submit**.

**Verify the number of records affected**

Each archive rule provides an estimate of the number of records the rule affects.

Role required: admin

This estimate only includes primary records and excludes any related records added to the archive rule. The estimate helps you determine if the archive rule affects the number of records you expect it to. If the estimate is too high or low, change the archive rule conditions and then click the **Recalculate Estimate** related link.

1. Navigate to **System Archiving > Archive Rules**.
2. Select the archive rule you want to estimate records for.
3. Click the **Recalculate Estimate** related link.

**Setting the language of archived strings**

On internationalized instances, the archive process uses the language of the **SYSTEM** user to select the display value strings.

If there is no **SYSTEM** user, the instance uses the default language setting to select the display value strings. You can either create a **SYSTEM** user with a specific language setting or set the system default language to **select the language of archived strings**.

**Create a destroy rule**

Create a destroy rule to delete archived records and related records after a specified amount of time.

Role required: admin

If you need to amend the destroy rule properties running against your archived data, see **Archive rule and destroy rule properties**.

1. Navigate to **System Archiving > Archive Destroy Rules**.
2. Click **New**.
3. Fill out the form fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Provide a descriptive name.</td>
</tr>
<tr>
<td>Table</td>
<td>Select the archive table that the system created when you archived records.</td>
</tr>
<tr>
<td>Description</td>
<td>Provide a description.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Destroy Related Records</td>
<td>Automatically destroy related records associated with the archived records.</td>
</tr>
<tr>
<td>Archive Duration</td>
<td>Specify the amount of time that records stay in the archive table before the system deletes them.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

5. You can check the archive destroy log at any time

**Archive rule and destroy rule properties**

Rules to prevent the archive process from consuming too many system resources have been automated.

In prior releases, you could set archive rules and deletion rules properties. This process has been automated, so that it is no longer necessary to adjust these parameters.

**Manage archived data**

You can view archived data, change an archive schedule, restore archived data, and archive a restored record.

Role required: admin
Use the following procedure to view archived data in the archive tables.

1. Navigate to **System Archiving > Archive Tables**.
2. Click the module name for the archived table you want to view. For example, **Archive Incidents**.

<table>
<thead>
<tr>
<th>Archived</th>
<th>Number</th>
<th>Opened at</th>
<th>Short description</th>
<th>Caller ID</th>
<th>Priority</th>
<th>State</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-05-14</td>
<td>INC0000039</td>
<td>2029-01-01 16:41:01</td>
<td>Trouble getting to Oregon mail server</td>
<td>Bud Richman</td>
<td>5 - Planning</td>
<td>Closed</td>
<td>Network</td>
</tr>
<tr>
<td>2020-05-14</td>
<td>INC0000041</td>
<td>2029-01-01 16:44:53</td>
<td>My desk phone does not work</td>
<td>Bob Ruggerli</td>
<td>3 - Moderate</td>
<td>Closed</td>
<td>Hardware</td>
</tr>
<tr>
<td>2020-05-14</td>
<td>INC0000009</td>
<td>2018-08-30 01:06:16</td>
<td>Unable to access the shared folder</td>
<td>David Miller</td>
<td>4 - Low</td>
<td>Closed</td>
<td>Inquiry / Help</td>
</tr>
<tr>
<td>2020-05-14</td>
<td>INC0000057</td>
<td>2016-08-10 09:14:59</td>
<td>Performance problems with wifi</td>
<td>Bertie Luby</td>
<td>5 - Planning</td>
<td>Closed</td>
<td>Inquiry / Help</td>
</tr>
<tr>
<td>2020-05-14</td>
<td>INC0000001</td>
<td>2018-05-11 20:36:26</td>
<td>Unable to post content on a Wiki page</td>
<td>David Miller</td>
<td>3 - Moderate</td>
<td>Closed</td>
<td>Inquiry / Help</td>
</tr>
</tbody>
</table>
3. Click a record from the archived table to see the archived record.
### Archive Incident: INC009001

<table>
<thead>
<tr>
<th>Number</th>
<th>Contact type</th>
</tr>
</thead>
<tbody>
<tr>
<td>INC009001</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Caller ID</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>David Miller</td>
<td>Closed</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Category</th>
<th>Hold reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inquiry / Help</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Subcategory</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2 - Medium</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Business service</th>
<th>Urgency</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2 - Medium</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service offering</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3 - Moderate</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CMDB CI</th>
<th>Assignment group</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Universal request</th>
<th>Assigned to</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Short description**: Unable to post content on a Wiki page

**Description**: I am not able to edit a wiki page.

**Notes**

<table>
<thead>
<tr>
<th>Notes</th>
<th>Related Records</th>
<th>Resolution Information</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Knowledge</th>
<th>Resolved by</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>System Administrator</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Close code</th>
<th>Resolved at</th>
</tr>
</thead>
<tbody>
<tr>
<td>Closed/Resolved by Caller</td>
<td>2020-05-14 14:21:05</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Close notes</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>logged in</td>
<td></td>
</tr>
</tbody>
</table>

**Related Links**

- Restore Record
- Restore Record and Related Records
- Show Archive Log Entry
Change an archive schedule

All active archive rules are executed by a system-scheduled job set to run every 60 minutes. You can modify the job if you need to change the interval.

Role required: admin

1. Navigate to System Scheduler > Scheduled Jobs.
2. Open the Archive record.
3. Modify the repeat value.

Restore archived records and related records

When you restore a record, the instance inserts it back into the primary table and flags the record as having been restored in the log. You can also restore the record along with related records.

Role required: admin

1. Navigate to System Archiving > Archive Log.
2. Select the archived record to restore.

```markdown
<table>
<thead>
<tr>
<th>Created</th>
<th>From table</th>
<th>To table</th>
<th>Display value</th>
<th>ID</th>
<th>Restored</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-05-13 02:06:45</td>
<td>sn_vul_vulnerable_item</td>
<td>ar_sn_vul_vulnerable_item</td>
<td>VIT0004681</td>
<td>Archive Vulnerable Item: VIT0004681</td>
<td>(empty)</td>
</tr>
<tr>
<td>2020-05-13 02:06:44</td>
<td>sn_vul_vulnerable_item</td>
<td>ar_sn_vul_vulnerable_item</td>
<td>VIT0004767</td>
<td>Archive Vulnerable Item: VIT0004767</td>
<td>(empty)</td>
</tr>
<tr>
<td>2020-05-13 02:06:44</td>
<td>sn_vul_vulnerable_item</td>
<td>ar_sn_vul_vulnerable_item</td>
<td>VIT0004767</td>
<td>Archive Vulnerable Item: VIT0004767</td>
<td>(empty)</td>
</tr>
<tr>
<td>2020-05-13 02:06:44</td>
<td>sn_vul_vulnerable_item</td>
<td>ar_sn_vul_vulnerable_item</td>
<td>VIT0004767</td>
<td>Archive Vulnerable Item: VIT0004767</td>
<td>(empty)</td>
</tr>
<tr>
<td>2020-05-13 02:06:44</td>
<td>sn_vul_vulnerable_item</td>
<td>ar_sn_vul_vulnerable_item</td>
<td>VIT0004806</td>
<td>Archive Vulnerable Item: VIT0004806</td>
<td>(empty)</td>
</tr>
<tr>
<td>2020-05-13 02:06:44</td>
<td>sn_vul_vulnerable_item</td>
<td>ar_sn_vul_vulnerable_item</td>
<td>VIT0004806</td>
<td>Archive Vulnerable Item: VIT0004806</td>
<td>(empty)</td>
</tr>
<tr>
<td>2020-05-13 02:06:44</td>
<td>sn_vul_vulnerable_item</td>
<td>ar_sn_vul_vulnerable_item</td>
<td>VIT0004806</td>
<td>Archive Vulnerable Item: VIT0004806</td>
<td>(empty)</td>
</tr>
<tr>
<td>2020-05-13 02:06:44</td>
<td>sn_vul_vulnerable_item</td>
<td>ar_sn_vul_vulnerable_item</td>
<td>VIT0004767</td>
<td>Archive Vulnerable Item: VIT0004767</td>
<td>(empty)</td>
</tr>
<tr>
<td>2020-05-13 02:06:44</td>
<td>sn_vul_vulnerable_item</td>
<td>ar_sn_vul_vulnerable_item</td>
<td>VIT0004767</td>
<td>Archive Vulnerable Item: VIT0004767</td>
<td>(empty)</td>
</tr>
<tr>
<td>2020-05-13 02:06:44</td>
<td>sn_vul_vulnerable_item</td>
<td>ar_sn_vul_vulnerable_item</td>
<td>VIT0004806</td>
<td>Archive Vulnerable Item: VIT0004806</td>
<td>(empty)</td>
</tr>
<tr>
<td>2020-05-13 02:06:44</td>
<td>sn_vul_vulnerable_item</td>
<td>ar_sn_vul_vulnerable_item</td>
<td>VIT0004806</td>
<td>Archive Vulnerable Item: VIT0004806</td>
<td>(empty)</td>
</tr>
</tbody>
</table>
```
3. Click the applicable related link:
   • Restore Record
   • Restore Record and Related Records
<xml version="1.0" encoding="UTF-8">
  <sn_vul_vulnerable_item>
    <active>true</active>
    <assignee>Brandon Ramirez</assignee>
    <created_at>2019-11-29T14:08:23Z</created_at>
    <closed_at>2019-11-29T14:08:23Z</closed_at>
    <updated_at>2019-11-29T14:08:23Z</updated_at>
    <display_val>"VR System"</display_val>
    <remaining_duration>0</remaining_duration>
    <assigned_to>"VR System"</assigned_to>
    <assignment_group>"VR System"</assignment_group>
    <assignment_rule>"VR System"</assignment_rule>
    <assignment_type>"VR System"</assignment_type>
    <business_criticality>"VR System"</business_criticality>
    <change_approval>"VR System"</change_approval>
    <cmdc_ci>"VR System"</cmdc_ci>
    <closed>"VR System"</closed>
    <detected_by חשבון מילאנו בוט יזואיס דבישב</detected_by>
    <description>"VR System"</description>
    <ignore_date>"VR System"</ignore_date>
    <ignore_reason>"VR System"</ignore_reason>
    <ignore_by>"VR System"</ignore_by>
    <integration_instance>"VR System"</integration_instance>
    <integration_run>"VR System"</integration_run>
    <ip_address>"VR System"</ip_address>
    <last_closed_by>"VR System"</last_closed_by>
    <last_closed_date>"VR System"</last_closed_date>
    <last_opened_by>"VR System"</last_opened_by>
    <last_opened_date>"VR System"</last_opened_date>
    <last_updated_by>"VR System"</last_updated_by>
    <last_updated_date>"VR System"</last_updated_date>
    <managed_by>"VR System"</managed_by>
    <managed_by_val>"VR System"</managed_by_val>
    <netbios>"VR System"</netbios>
    <number>"VR System"</number>
    <opened_at>"VR System"</opened_at>
    <opened_by>"VR System"</opened_by>
    <opened_date>"VR System"</opened_date>
    <reopened>"VR System"</reopened>
    <reopened_date>"VR System"</reopened_date>
    <risk_rating>"VR System"</risk_rating>
    <risk_score>"VR System"</risk_score>
    <security_tags>"VR System"</security_tags>
    <short_description>"VR System"</short_description>
  </sn_vul_vulnerable_item>
</xml>
Warning: Do not delete archive record log entries. Deleting an archive log entry prevents you from restoring the data for the archived records.

Archive a restored record

You can automatically re-archive a restored record or you can manually archive the record.

Role required: admin

1. Navigate to the restored record.
2. Click the **Archive Record** link.
**Incident INCO009001**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>INCO009001</td>
</tr>
<tr>
<td>Caller</td>
<td>David Miller</td>
</tr>
<tr>
<td>Category</td>
<td>Inquiry / Help</td>
</tr>
<tr>
<td>Subcategory</td>
<td>-- None --</td>
</tr>
<tr>
<td>Service</td>
<td>-- None --</td>
</tr>
<tr>
<td>Service offering</td>
<td></td>
</tr>
<tr>
<td>Configuration item</td>
<td></td>
</tr>
<tr>
<td>Contact type</td>
<td>-- None --</td>
</tr>
<tr>
<td>State</td>
<td>Closed</td>
</tr>
<tr>
<td>Impact</td>
<td>2 - Medium</td>
</tr>
<tr>
<td>Urgency</td>
<td>2 - Medium</td>
</tr>
<tr>
<td>Priority</td>
<td>3 - Moderate</td>
</tr>
<tr>
<td>Short description</td>
<td>Unable to post content on a Wiki page</td>
</tr>
<tr>
<td>Description</td>
<td>I am not able to edit a wiki page.</td>
</tr>
</tbody>
</table>

**Notes**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problem</td>
<td></td>
</tr>
<tr>
<td>Change Request</td>
<td></td>
</tr>
<tr>
<td>Caused by Change</td>
<td></td>
</tr>
</tbody>
</table>

**Related Links**

- Archive Record
- Repair SLAs
Data archive table size limits

There are constraints to the size of the table you use to archive your instance data.

Limits on data archive tables

There is a limit on the size of an archive table you can create to store data. If you receive an error that an archive table could not be created, it might be related to this size limitation.

<table>
<thead>
<tr>
<th>Archive table size limits</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Table Attribute</strong></td>
</tr>
<tr>
<td>Single table static size limit</td>
</tr>
<tr>
<td>Rowsize limit</td>
</tr>
</tbody>
</table>

You can follow KB0689595 to reduce the size of a table you need to archive by identifying unused columns and converting large varchar fields into mediumtext fields, but you might then encounter a rowsize limitation. You can address a rowsize limitation in the TPP hierarchy by migrating fields to another partition table. However, you are attempting to create a single archive table which has all the fields for the table spread over two or more partition tables. Creating this single archive table can result in a table which still exceeds the overall table size limit.

If you cannot create an archive table after reducing the size to meet the table limits, please contact Customer Service and Support.

Data migration process for archiving table data from non-reference fields to reference fields

The data migration process moves data from an existing archive table, including descendent and related tables. There are special scripts and notes to understand when completing this process.

Data migration job (RefCopyJob)

For each table that goes through the migration process, the **RefCopyJob** identifies the sys_id of the reference fields and updates the display value to be the correct sys_id. The job configures 10k records at a time unless there are more than 10k records with the same timestamp. The migration progress relies on the archived timestamp. The script determines the tables to migrate:

```javascript
var tables = GlideDBObjectManager.get().getAllExtensions(current.table);
for (i = 0; i < tables.size(); i++) {
  var gr = new GlideRecord('sys_archive_ref_migration');
  gr.addQuery('table', 'ar_' + tables.get(i));
  gr.query();
  if (!gr.next()) {
    if (GlideTableDescriptor.isValid('ar_' + tables.get(i))) {
      var gr2 = new GlideRecord("sys_archive_ref_migration");
      gr2.initialize();
      gr2.setValue('rule', current.sys_id);
      gr2.setValue('table', 'ar_' + tables.get(i));
      gr2.setValue('reference_migration_progress', 'waiting');
      gr2.insert();
    }
  }
}
//Also get insert related records tables as well
```
var map = new GlideRecord('sys_archive');
map.addQuery('table', current.table);
map.query();
if (map.next()) {
    var id = map.getValue('sys_id');
    if (!(id === undefined)) {
        var related = new GlideRecord('sys_archive_related');
        related.addQuery('archive_map', id);
        related.addQuery('action', 'archive');
        related.query();
        while (related.next()) {
            if (!GlideTableDescriptor.isValid('ar_' +
                related.getValue('table'))) {
                gs.log('Related Record table: ' +
                    related.getValue('table') + ' not created yet');
                continue;
            }
            var gr3 = new GlideRecord("sys_archive_ref_migration");
            gr3.initialize();
            gr3.setValue('rule', current.sys_id);
            gr3.setValue('table', 'ar_' + related.getValue('table'));
            gr3.setValue('reference_migration_progress', 'waiting');
            gr3.insert();
        }
    }
}

Change the sys_dictionary types of migrated tables job (ArchiveRefJob)

After the tables associated with an archive rule completely migrate, the ArchiveRefJob job executes. This job changes
the sys_dictionary types of the archive table from String to Reference.

Fixing node failures for RefCopyJob and ArchiveRefJob

If node failure occurs while these jobs are running, it leaves the status of the data migration in an improper state. If
the RefCopyJob fails, it can leave a table in a migrating status. You can verify this condition by checking if rows in
the sys_archive_ref_migration are stuck in migrating status for an extraordinary amount of time (quantify?). Update
the specific row status from migrating to waiting and the RefCopyJob continues the data migration on the table
when the job runs again.

The node can also fail when the ArchiveRefJob terminates prematurely. Check if tables have fields that are
reference fields and some that are still string type fields. The job might have died in the middle of changing the field
types. You can resolve this condition by setting up a trigger job to execute in a background script which starts the
process over again:

GlideRecord trigger = new GlideRecord(SYS_TRIGGER);
trigger.initialize();
trigger.setValue('state', 0);
trigger.setValue('trigger_type', 0);
trigger.setValue('next_action', new GlideDateTime());
trigger.setValue('job_context', 'fcRuleId=' + ruleId);
trigger.setValue('name', 'Job Reference Migration' + ' Node - ' + new
    GlideClusterSynchronizer().getSystemID());
trigger.setValue('trigger_class',
    com.glide.db.auxiliary.job.ArchiveRefJob);
trigger.insert();
Export and import XML files

To occasionally migrate data from one instance to another, you can export XML data from one instance and import it to another.

This method ensures that all fields and values are transferred exactly. Migrating data in an XML file saves time for unscheduled data imports because there is no need to build an import set or a transform map.

Exporting and importing data in XML files is commonly used for records created in a development instance that must be migrated with the update sets as part of a migration procedure. Examples of these records include lookup tables, unit test records, and other information required to support production. Typically, this information is only migrated once and the overhead of an import set is not justified.

Note: Image field data is not preserved when exporting to XML.

Exporting data

There are a variety of ways for administrators and users to export data.

Form export
Export an individual record from the user interface. Choose PDF or XML format directly from a form.

List export
Export multiple records from the user interface. Choose CSV, Excel, PDF, or XML format directly from a list.

URL export
Export multiple records from a table using the CSV, Excel, PDF, or XML processor. Specify the table form or list you want to export in the URL.

Web services
Export multiple records from a table when an external client makes a web services request. Create an external application or process to automate the retrieval of data from an instance via web services such as REST or SOAP.

Export sets
Create a file called an export set that contains all the data you want to export.
## Export formats

### Available export formats

<table>
<thead>
<tr>
<th>Export format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSV</td>
<td>Export table records as a comma-separated value text file. Use this option to export the currently displayed fields in the list or form as a text file. Configure the list or form to add or remove fields from the export. When exported to CSV, dot-walked fields appear using their full field name, such as u_assignment_group.parent.</td>
</tr>
</tbody>
</table>

**Note:** By default, ServiceNow exports all CSV files in Windows-1252 encoding. If you need to export translated data, set the `glide.export.csv.charset` system property to UTF-8.

| Excel         | Export table records as a Microsoft Excel spreadsheet. Use this option to export the currently displayed fields in the list or form as an Excel spreadsheet. Configure the list or form to add or remove fields from the export. |

| XML           | Export table records as an XML document. Use this option to export all data from a table or all data for a particular record. The XML file has an XML element for each column in the table. |

**Note:** Image field data is not preserved when exporting to XML.

| PDF           | Export table records as a Portable Document Format file. Use this option to export the currently displayed fields in the list or form as a PDF file. Configure the list or form to add or remove fields from the export. |

**Note:** The PDF export processor prints data from left-to-right, which can produce rendering errors when displaying right-to-left language data.

| JSON          | Export the table records as a JSON string. The JSON file has an element for each column in the table. |

### Column headers

The file type you export to, such as CSV or PDF determines how column headers are exported. In general, formats meant for human consumption such as PDF display the column label, whereas formats meant for machine use such as CSV use the database field_name.
## Header format by file type

<table>
<thead>
<tr>
<th>File type</th>
<th>Column header format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Excel</td>
<td>Label</td>
</tr>
<tr>
<td>PDF</td>
<td>Label</td>
</tr>
<tr>
<td>CSV</td>
<td>field_name</td>
</tr>
<tr>
<td>XML</td>
<td>field_name</td>
</tr>
<tr>
<td>JSON</td>
<td>field_name</td>
</tr>
</tbody>
</table>

## Export limits

The platform provides a default upper limit for data exports.

The purpose of the upper limit is to avoid creating performance issues when a table is excessively large. If you need to export more records than the threshold permits, Break up a large export into separate manageable chunks.

## Export limit properties

You can set the number of records to return during an export using the `sysparm_record_count` URL parameter. However, the system analyzes the following settings to determine whether an export limit should be applied.

1. First, the platform checks the property that defines the format-specific export limit (see table below). Each format can have a different limit. Although this property can be set to any value, exceeding the default export limit can impact system performance. You may want to set the property at or below the default limit and have users Break up a large export to export large amounts of data.

2. If the format-specific property is not set, the system checks the property for the general export limit (see table below). This property can also be set to any value, but exceeding the default export limit can impact system performance.

3. If neither the format-specific export limit nor the general export limit property is set, the system enforces the default export limit (see table below).

### Important: To set these properties, navigate to System Properties > Import Export.

## Default export limit

<table>
<thead>
<tr>
<th>Format</th>
<th>Format-specific export limit</th>
<th>General export limit</th>
<th>Default export limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>XML</td>
<td>glide.xml.export.limit</td>
<td>glide.ui.export.limit</td>
<td>10,000</td>
</tr>
<tr>
<td>CSV</td>
<td>glide.csv.export.limit</td>
<td>glide.ui.export.limit</td>
<td>10,000</td>
</tr>
<tr>
<td>EXCEL (XLSX)</td>
<td>glide.xlsx.export.limit</td>
<td>glide.ui.export.limit</td>
<td>10,000</td>
</tr>
<tr>
<td>EXCEL (XLS)</td>
<td>glide.excel.export.limit</td>
<td>glide.ui.export.limit</td>
<td>10,000</td>
</tr>
<tr>
<td>EXCEL (XLSX)</td>
<td>glide.xlsx.max_cells</td>
<td>N/A</td>
<td>500,000</td>
</tr>
<tr>
<td>EXCEL (XLS)</td>
<td>glide.excel.max_cells</td>
<td>N/A</td>
<td>500,000</td>
</tr>
</tbody>
</table>
### Export limit examples

<table>
<thead>
<tr>
<th>Example</th>
<th>Property</th>
<th>Table</th>
<th>Note</th>
</tr>
</thead>
</table>
| Exporting to CSV | • glide.csv.export.limit = 20,000  
• glide.ui.export.limit = 10,000  
• com.glide.processors.XMLProcessor.max_record_count = 20,000  
• Default export limit for CSV = 10,000 | ![Table](#) | In the second export, the number of records returned from the database is limited because the number of records specified for export exceeds the value set in the glide.csv.export.limit property. |

---

**Note:**
- The number of rows can be set from 0 to 5,000. If no value is specified, the default is 1,000. If a value greater than 5,000 is specified, the default value of 1,000 is used.
- Although the number of columns can be set higher than 25, this is not advisable, since only 25 header labels fit on a page.
### Excel export threshold

Excel exports are intended for relatively small exports, fewer than 500,000 cells, while CSV can handle larger exports.

Whenever you export to Excel and the resultant spreadsheet has more than 500,000 cells (by default), the export process stops and you are given the Excel file at that point. In the bottom row, there will be the following message: Export stopped due to excessive size. Use CSV for a complete export:

```
    1       A          B          C          D
      1  Table Column name Text index Calculated Reason
16848  16848 cmdb_tcp_half sys_mod_count   FALSE       FALSE
16849  16849 cmdb_tcp_half sys_created_on  FALSE       FALSE
16850  16850 cmdb_tcp_half sys_created_by  FALSE       FALSE
16851  16851 cmdb_tcp_half sys_modified   FALSE       FALSE
16852  16852 Export stopped due to excessive size. Use CSV for a complete export.
16853
```

### Excel export threshold

The Excel export cell threshold is customizable using the `glide.xlsx.max_cells` integer property (or `glide.excel.max_cells` if using XLS).
**Note:** Increasing this threshold may cause a memory issue in your instance. The threshold is set at an appropriate level to prevent resource issues.

The export will put the information into the Excel document with 32,000 rows per spreadsheet.

**Form export**

Any user role can export form data in a variety of formats.

Export formats include:

- PDF (Portrait)
- PDF (Landscape)
- XML (This Record)

Export an individual record from a form by right-clicking a form header bar and selecting the export type.

Export from form

**Note:** When exporting PDF data from a form, any field that is disabled by UI scripts (UI policies, UI actions, client scripts) and any fields that are visible from the current view, are exported. However, when
exporting XML data, all of the fields are exported, regardless of the view. You cannot export records to CSV or Excel from a form.

When exporting to XML, a dialog box may prompt you to save the file, or the browser may automatically save the XML file to the downloads folder specified in the browser preferences.

**List export**

You can export a list of records in a variety of formats.

The Export option is available in the column heading context menu in List v2. In List v3, it is available in the list title menu.
Note: To export records in an embedded list, export the record containing the list.

Export formats include:

- Excel
- CSV
- XML
- JSON
- PDF (Portrait)
- PDF (Landscape)
- PDF (Detailed Portrait): Exports the list and the associated form for each record.
- PDF (Detailed Landscape): Exports the list and the associated form for each record.

Note: You can control how line breaks appear in exported CSV data using the glide.csv.export.line_break system property.

Note: To remove unwanted HTML tags from list data, see the blog Rendering HTML in Exported Lists by a ServiceNow employee in the Now Community.

When exporting to XML, a dialog box may prompt you to save the file, or the browser may automatically save the XML file to the downloads folder specified in the browser preferences.

Determining which list fields are exported

By default, exporting data from a list exports only the fields that are visible from the current view.

By default, exporting data from a list exports only the fields that are visible from the current view. If you want to export fields from another list view, you can switch views from the UI. Alternatively, you can add the sysparm_view parameter to the URL request. For example, to export fields visible from the Self Service (ess) view:

https://instance_name.service-now.com/incident.do?CSV&sysparm_view=ess

If you are exporting CSV or Excel data and do not specify a view, the export uses the default list view. You can export all fields by setting the sysparm_default_export_fields parameter to all. If you are exporting XML data, the export returns all fields unless you specify a particular view. The sysparm_default_export_fields parameter has no effect on XML exports.

Use a URL query to filter a list result

Use URL queries to programmatically generate filtered lists before exporting them.

URL queries are useful for scripts that generate a list of records and where no user will manually add the filter from the UI. You must be familiar with the table's column names and values to create a query.

1. Specify the instance URL. For example, https://demo.service-now.com/.
2. Specify the list URL for the table you want to export. For example, incident_list.do.
3. Specify the export format processor for the export. For example, ?XML.
4. Specify the query as the value of the sysparm_query parameter. For example, ?sysparm_query=priority=1.
5. Optional: Specify the result sort order with the sysparm_orderby= parameter. For example, CSV&sysparm_orderby=assigned_to.

Note: All queries use a column name, an operator, and a value. See Condition Builder for a list of available operators.

For example, to export a list of all priority 1 incidents as an XML file, use the following URL: https://<instance_name>.service-now.com/incident_list.do?XML&sysparm_query=priority=1&sysparm_orderby=assigned_to
Export controls

Control the column value and header value in export files using query parameters, export set properties, and system properties.

Depending on the output formats you prefer, you can use export controls to do the following:

- Export column values as either display values (for example, `Assignment group = Network`) or raw values (for example, `Assignment Group = 287ebd7da9fe198100f92cc8d1d2154e`).
- Export table headings as either heading labels (for example, `Assignment Group`) or heading names (for example, `assignment_group`).

Query parameters for display value and header

Use query parameters to export the display value or raw value of fields and the field label or field name for headers.

Query parameters control the output for CSV, Excel, JSON, XLSX, and XML file formats. Query parameters, if present, override system properties.

The following table describes each of the query parameters that control display values and headers.

<table>
<thead>
<tr>
<th>Query parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sysparm_display_value</td>
<td>Exports the display value (true) or raw value (false) for the CSV, Excel, XLSX, and XML file formats. See Field types affected by export controls for more information.</td>
</tr>
<tr>
<td>displayvalue</td>
<td>Exports the display value (true), raw value (false), or both (All) for the JSON file format. See Field types affected by export controls for more information.</td>
</tr>
<tr>
<td>sysparm_export_column_header_label</td>
<td>Exports the CSV, Excel, and XLSX file formats with the field label (true) or field name (false).</td>
</tr>
</tbody>
</table>

**sysparm\_display\_value**

**Example:**

```
sysparm\_display\_value = true
```

<table>
<thead>
<tr>
<th>Number</th>
<th>Opened</th>
<th>Short description</th>
<th>Caller</th>
<th>State</th>
<th>Assignment group</th>
<th>Assigned to</th>
</tr>
</thead>
<tbody>
<tr>
<td>INC0000060</td>
<td>2016-12-07 17:19:57</td>
<td>Unable to connect to email</td>
<td>Joe Employee</td>
<td>Closed</td>
<td>Network</td>
<td>David Loo</td>
</tr>
<tr>
<td>INC0000059</td>
<td>2016-08-10 09:14:29</td>
<td>Unable to access team file share</td>
<td>Rick Berzle</td>
<td>New</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INC0000058</td>
<td>2016-08-10 09:37:45</td>
<td>Performance problems with email</td>
<td>Bow Uggerg</td>
<td>New</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INC0000057</td>
<td>2016-08-10 09:14:59</td>
<td>Performance problems with wifi</td>
<td>Bertie Luby</td>
<td>New</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INC0000055</td>
<td>2017-09-09 21:47:23</td>
<td>SAP Sales app is not accessible</td>
<td>Carol Coughlin</td>
<td>In Progress</td>
<td>Service Desk</td>
<td>Beth Anglin</td>
</tr>
</tbody>
</table>

**Example:**

```
sysparm\_display\_value = false
```

© 2021 ServiceNow, Inc. All rights reserved.
displayvalue

Example:

displayvalue = true

```
{  
  "records": [  
    {  
      "parent": "",  
      "made_sla": "false",  
      "caused_by": "",  
      "watch_list": "",  
      "upon_reject": "null",  
      "sys_updated_on": "2017-10-11 13:16:07",  
      "child_incidents": "",  
      "hold_reason": "",  
      "approval_history": "",  
      "number": "INC0000001",  
      "resolved_by": "System Administrator",  
      "sys_updated_by": "admin",  
      "opened_by": "Joe Employee"  
    }  
  ]
}
```

Example:

displayvalue = false
Example:

displayvalue = All

Example:

sysparm_export_column_header_label

displayvalue = true
Example:

sysparm_export_column_header_label = false

Export Set fields for display value and header

Use Export Set fields to export the display value or raw value of fields and the field label or field name for headers.

Export Set fields control the output for the CSV, Excel, JSON, XLSX, and XML file formats. Export Set fields, if present, override system properties.

The following table describes each of the Export Set fields that control display values and headers.

<table>
<thead>
<tr>
<th>Export Set Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Column headers</strong></td>
<td>Exports the CSV, Excel, and XLSX file formats with the field label (Use field label) or field name (Use field name).</td>
</tr>
</tbody>
</table>
| **Column values**        | Exports the display value (Use display value) or raw value (Use raw value) for the CSV, Excel, JSON, XLSX, and XML file formats.  
                           | See Field types affected by export controls for more information.             |

Column headers

Example:

Use field label

Example:
Use field name

<table>
<thead>
<tr>
<th>Number</th>
<th>Opened</th>
<th>Short description</th>
<th>Caller</th>
<th>State</th>
<th>Assignment group</th>
<th>Assigned to</th>
</tr>
</thead>
<tbody>
<tr>
<td>INC00000060</td>
<td>2016-12-12 07:19:57</td>
<td>Unable to connect to email</td>
<td>Joe Employee</td>
<td>Closed</td>
<td>Network</td>
<td>David Loo</td>
</tr>
<tr>
<td>INC00000059</td>
<td>2016-08-10 09:14:29</td>
<td>Unable to access team file share</td>
<td>Rick Berzle</td>
<td>New</td>
<td>New</td>
<td></td>
</tr>
<tr>
<td>INC00000058</td>
<td>2016-08-10 09:37:45</td>
<td>Performance problems with email</td>
<td>Bow Ruggier</td>
<td>New</td>
<td>New</td>
<td></td>
</tr>
<tr>
<td>INC00000057</td>
<td>2016-08-10 09:14:59</td>
<td>Performance problems with wifi</td>
<td>Bertie Luby</td>
<td>New</td>
<td>New</td>
<td></td>
</tr>
<tr>
<td>INC00000055</td>
<td>2017-09-20 21:47:23</td>
<td>SAP Sales app is not accessible</td>
<td>Carol Coughlin</td>
<td>In Progress</td>
<td>Service Desk</td>
<td>Beth Anglin</td>
</tr>
</tbody>
</table>

Column values

Example:
Use display value

<table>
<thead>
<tr>
<th>Number</th>
<th>Opened</th>
<th>Short description</th>
<th>Caller</th>
<th>State</th>
<th>Assignment group</th>
<th>Assigned to</th>
</tr>
</thead>
<tbody>
<tr>
<td>INC00000060</td>
<td>2016-12-12 07:19:57</td>
<td>Unable to connect to email</td>
<td>Joe Employee</td>
<td>Closed</td>
<td>Network</td>
<td>David Loo</td>
</tr>
<tr>
<td>INC00000059</td>
<td>2016-08-10 09:14:29</td>
<td>Unable to access team file share</td>
<td>Rick Berzle</td>
<td>New</td>
<td>New</td>
<td></td>
</tr>
<tr>
<td>INC00000058</td>
<td>2016-08-10 09:37:45</td>
<td>Performance problems with email</td>
<td>Bow Ruggier</td>
<td>New</td>
<td>New</td>
<td></td>
</tr>
<tr>
<td>INC00000057</td>
<td>2016-08-10 09:14:59</td>
<td>Performance problems with wifi</td>
<td>Bertie Luby</td>
<td>New</td>
<td>New</td>
<td></td>
</tr>
<tr>
<td>INC00000055</td>
<td>2017-09-20 21:47:23</td>
<td>SAP Sales app is not accessible</td>
<td>Carol Coughlin</td>
<td>In Progress</td>
<td>Service Desk</td>
<td>Beth Anglin</td>
</tr>
</tbody>
</table>

Example:
Use raw value

<table>
<thead>
<tr>
<th>Number</th>
<th>Opened</th>
<th>Short description</th>
<th>Caller</th>
<th>State</th>
<th>Assignment group</th>
<th>Assigned to</th>
</tr>
</thead>
<tbody>
<tr>
<td>INC00000060</td>
<td>2016-12-12 15:19:57</td>
<td>Unable to connect to email</td>
<td>681aca9b0a016409b9a026818a9757c7</td>
<td>Closed</td>
<td>Network</td>
<td>David Loo</td>
</tr>
<tr>
<td>INC00000059</td>
<td>2016-08-10 16:14:29</td>
<td>Unable to access team file share</td>
<td>5137f53c611227d0800109f92e8a015a</td>
<td>New</td>
<td>New</td>
<td></td>
</tr>
<tr>
<td>INC00000058</td>
<td>2016-08-10 16:37:45</td>
<td>Performance problems with email</td>
<td>5293626b1612229ab60dce754bc8</td>
<td>New</td>
<td>New</td>
<td></td>
</tr>
<tr>
<td>INC00000057</td>
<td>2016-08-10 16:14:59</td>
<td>Performance problems with wifi</td>
<td>7a32f50371020004e68b8e56377</td>
<td>New</td>
<td>New</td>
<td></td>
</tr>
<tr>
<td>INC00000055</td>
<td>2017-09-21 04:47:23</td>
<td>SAP Sales app is not accessible</td>
<td>46c1293809f2181003dc753e7b9bee</td>
<td>In Progress</td>
<td>Service Desk</td>
<td>Beth Anglin</td>
</tr>
</tbody>
</table>

System properties for display value and header

Use system properties to export the display value or raw value of fields and the field label or field name for headers.

System properties control the output for the CSV, Excel, JSON, and XLSX file formats. System properties define default behavior if overrides such as query parameters are not specified. System properties apply to exported files downloaded with URL parameters, exported from list view, or generated by export sets.

The following table describes each of the system properties that control display values and headers.

<table>
<thead>
<tr>
<th>Format</th>
<th>Property</th>
<th>Default Value</th>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSV</td>
<td>glide.export.csv.raw.value</td>
<td>false</td>
<td>Setting the property as false also crops the value's string to 32000 characters.</td>
</tr>
<tr>
<td></td>
<td>glide.export.csv.column_header_label</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Format</td>
<td>Property</td>
<td>Default Value</td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>----------------------------------------------</td>
<td>---------------</td>
<td></td>
</tr>
<tr>
<td>Excel</td>
<td>glide.export.excel.display_value</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td></td>
<td>glide.export.excel.column_header_label</td>
<td></td>
<td></td>
</tr>
<tr>
<td>JSON</td>
<td>glide.json.return_displayValue</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>XLSX</td>
<td>glide.export.xlsx.display_value</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td></td>
<td>glide.export.xlsx.column_header_label</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**CSV**

Example:

```plaintext
glide.export.csv.raw.value = false  (default)
glide.export.csv.column_header_label = false  (default)
```

<table>
<thead>
<tr>
<th>number</th>
<th>opened_at</th>
<th>short_description</th>
<th>caller_id</th>
<th>state</th>
<th>assignment_group</th>
<th>assigned_to</th>
</tr>
</thead>
<tbody>
<tr>
<td>INC0000060</td>
<td>12/12/16 7:19</td>
<td>Unable to connect to email</td>
<td>Joe Employee</td>
<td>Closed</td>
<td>Network</td>
<td>David Loo</td>
</tr>
<tr>
<td>INC0000059</td>
<td>8/10/16 9:14</td>
<td>Unable to access team file share</td>
<td>Rick Berzle</td>
<td>New</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INC0000058</td>
<td>8/10/16 9:37</td>
<td>Performance problems with email</td>
<td>Bow Ruggeri</td>
<td>New</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INC0000057</td>
<td>8/10/16 9:14</td>
<td>Performance problems with wifi</td>
<td>Bertie Luby</td>
<td>New</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INC0000055</td>
<td>9/20/17 21:47</td>
<td>SAP Sales app is not accessible</td>
<td>Carol Coughlin</td>
<td>In Progress</td>
<td>Service Desk</td>
<td>Beth Anglin</td>
</tr>
</tbody>
</table>

Example:

```plaintext
glide.export.csv.raw.value = true
glide.export.csv.column_header_label = true
```

<table>
<thead>
<tr>
<th>Number</th>
<th>opened</th>
<th>short_description</th>
<th>caller</th>
<th>state</th>
<th>assignment group</th>
<th>assigned_to</th>
</tr>
</thead>
<tbody>
<tr>
<td>INC0000060</td>
<td>12/12/15 15:19</td>
<td>Unable to connect to email</td>
<td>6816ca5f9da0a1640019a6818e57c7</td>
<td>1 287bf37a0f19810391492e025fe052d065</td>
<td>2a7b62c37e11227dd0b9b8ed7a4c37</td>
<td></td>
</tr>
<tr>
<td>INC0000059</td>
<td>8/10/16 16:14</td>
<td>Unable to access team file share</td>
<td>51397f5c6f12112727d0b8ed7a4c37</td>
<td>1 287bf37a0f19810391492e025fe052d065</td>
<td>2a7b62c37e11227dd0b9b8ed7a4c37</td>
<td></td>
</tr>
<tr>
<td>INC0000058</td>
<td>8/10/16 16:37</td>
<td>Performance problems with email</td>
<td>2983b264d11227b01064c6b7f9134c8</td>
<td>1 287bf37a0f19810391492e025fe052d065</td>
<td>2a7b62c37e11227dd0b9b8ed7a4c37</td>
<td></td>
</tr>
<tr>
<td>INC0000057</td>
<td>8/10/16 16:14</td>
<td>Performance problems with wifi</td>
<td>76db0a3b37120200400f8f8bc3b62e37</td>
<td>1 287bf37a0f19810391492e025fe052d065</td>
<td>2a7b62c37e11227dd0b9b8ed7a4c37</td>
<td></td>
</tr>
<tr>
<td>INC0000055</td>
<td>9/24/17 6:47</td>
<td>SAP Sales app is not accessible</td>
<td>46c1291a2f6a3944781000e066e79e5e63</td>
<td>2 2a7b62c37e11227dd0b9b8ed7a4c37</td>
<td>2a7b62c37e11227dd0b9b8ed7a4c37</td>
<td></td>
</tr>
</tbody>
</table>

**Excel**

Example:

```plaintext
glide.export.excel.display_value = true  (default)
glide.export.excel.column_header_label = true  (default)
```

© 2021 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Example:

```plaintext
.glide.export.excel.display_value = false
.glide.export.excel.column_header_label = false
```

**JSON**

Example:

```plaintext
.glide.json.return_displayValue = false (default)

```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}```
```{}````

Example:

```plaintext
.glide.json.return_displayValue = true
```

**XLSX**

Example:

```plaintext
.glide.export.xlsx.display_value = true (default)
.glide.export.xlsx.column_header_label = true (default)
```
Example:

```plaintext
glide.export.xlsx.display_value = false  
glide.export.xlsx.column_header_label = false
```

Field types affected by export controls

Different field types are affected differently by export controls.

The following table describes how different field types are affected by export controls.

<table>
<thead>
<tr>
<th>Field type</th>
<th>Display value</th>
<th>Raw value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date/Time</td>
<td>CSV: User timezone date/time with user format.</td>
<td>CSV: UTC timezone date/time with system format.</td>
</tr>
<tr>
<td></td>
<td>Excel/XLSX: User timezone date/time with user format if <code>glide.excel.use_user_date_format</code> set, otherwise system format.</td>
<td>Excel/XLSX: UTC timezone date/time with user format if <code>glide.excel.use_user_date_format</code> set, otherwise system format.</td>
</tr>
<tr>
<td>Date</td>
<td>Date with user format.</td>
<td>Date with system format.</td>
</tr>
<tr>
<td></td>
<td>Excel/XLSX: Date with user format if <code>glide.excel.use_user_date_format</code> set, otherwise system format.</td>
<td>Excel/XLSX: Date with user format if <code>glide.excel.use_user_date_format</code> set, otherwise system format.</td>
</tr>
<tr>
<td>Time</td>
<td>CSV: Time with user format.</td>
<td>CSV: UTC time, assuming 1970-01-01 as the date with system format.</td>
</tr>
<tr>
<td></td>
<td>Excel/XLSX: User timezone time with user format if <code>glide.excel.use_user_date_format</code> set, otherwise system format.</td>
<td>Excel/XLSX: UTC time, assuming 1970-01-01 as the date with user format if <code>glide.excel.use_user_date_format</code> set, otherwise system format.</td>
</tr>
<tr>
<td>References</td>
<td>Display value of the referenced record.</td>
<td>Sys_id of the referenced record.</td>
</tr>
<tr>
<td>Choice</td>
<td>Label of the selected choice.</td>
<td>Value of the selected choice.</td>
</tr>
<tr>
<td>Currency</td>
<td>Value with the currency symbol.</td>
<td>USD value without the currency symbol.</td>
</tr>
<tr>
<td>Field type</td>
<td>Display value</td>
<td>Raw value</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>Price (calculated)</td>
<td>Value with the currency symbol.</td>
<td>USD value without the currency symbol.</td>
</tr>
<tr>
<td>Price (fixed)</td>
<td>Value with the currency symbol.</td>
<td>USD value without the currency symbol.</td>
</tr>
</tbody>
</table>

**Default values for column headers and column values**

Default values are used for column headers and column values, unless overridden by query parameters, Export Set fields, or system properties.

The following table describes the default values used if you do not use query parameters, Export Set fields, or system properties to control output format.

<table>
<thead>
<tr>
<th>Output format</th>
<th>Column headers</th>
<th>Column values</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSV</td>
<td>Use field name</td>
<td>Use raw value if glide.export.csv.raw.value set, otherwise Use display value.</td>
</tr>
<tr>
<td>Excel</td>
<td>Use field label</td>
<td>Use display label</td>
</tr>
<tr>
<td>JSON</td>
<td>N/A</td>
<td>Use raw value</td>
</tr>
<tr>
<td>XLSX</td>
<td>Use field label</td>
<td>Use display value</td>
</tr>
<tr>
<td>XML</td>
<td>N/A</td>
<td>Use raw value</td>
</tr>
</tbody>
</table>

**Exporting currency fields to Excel**

Exporting currency fields to Excel applies Account formatting and can be configured to convert all values to US dollars or to export values in the user's session currency.

When exporting currency fields to Microsoft Excel, the cells containing currency data use Accounting formatting. This formatting allows you to perform numeric operations on those values as well as view the currency symbol, such as $ or €.

When exporting currency fields the type of currency, such as $ or €, is preserved by default. The conversion rates for non-USD currencies are stored on the Exchange Rates [fx_rate] table.

You can choose to export all currency values either in US dollars or in the user's session currency.

- To export all currency values in US dollars, set the property `glide.excel.fixed_currency_usd` to `true`.
- To export all currency values in the user's session currency, set the property `glide.excel.convert_to_user_currency` to `true`.

If both `glide.excel.fixed_currency_usd` and `glide.excel.convert_to_user_currency` are set to `true`, `glide.excel.fixed_currency_usd` overrides `glide.excel.convert_to_user_currency`.

**Currency export behavior and symbols**

The behavior of the currency field in Excel depends on the Symbol of the currency.

- When the currency symbol is $, the Excel cell type is set as Currency.
- When the currency symbol is 1 character (such as ¥ or €) or more than 1 character (such as KR), the Excel cell type is set to Custom.
Export directly from a URL

You may want to export data from the URL if you need to dynamically export data from a script or web service.

You must be familiar with the ServiceNow table and column names to export data directly from the URL. See Navigate to a record or a module using a URL for more information about navigating to forms and lists.

Query parameters are available for you to use in the instance URL so you can display a specific list of records in a specific order:

<table>
<thead>
<tr>
<th>URL Parameter</th>
<th>URL Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sysparm_query</td>
<td>sysparm_query=[column name] [operator][value]</td>
<td>Displays a list of records that match the query. For example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>https://&lt;instance name&gt;.service-now.com/incident_list.do?XML&amp;sysparm_query=priority=1</td>
</tr>
<tr>
<td>sysparm_orderby</td>
<td>sysparm_orderby=[column name]</td>
<td>Sorts a list of records by the column name provided. For example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>https://&lt;instance name&gt;.service-now.com/incident_list.do?XML&amp;sysparm_query=priority=1&amp;sysparm_orderby=assigned_to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can sort by only one column using sysparm_orderby. To sort by multiple columns, use sysparm_query=ORDERBY[column name]^ORDERBY[column name]. For example: sysparm_query=ORDERBYassigned_to^ORDERBYpriority.</td>
</tr>
</tbody>
</table>

To export data directly from the URL, create a URL containing the following parts:

1. Specify the instance URL. For example, https://<instance name>.service-now.com/.
2. Specify the table form or list to export. For example, incident_list.do.
3. Specify the export format processor to use for the export. For example, ?CSV.
4. Optional: Specify a query and sort order with URL parameters. For example, &sysparm_query=sys_id%3E%3Db4aedb520a0a0b1001af10e278657d27.

The final URL should look like one of these sample URLs:

<table>
<thead>
<tr>
<th>URL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>https://&lt;instance name&gt;.service-now.com/incident_list.do?CSV&amp;sysparm_query=sys_id%3E%3Db4aedb520a0a0b1001af10e278657d27</td>
<td>Export a particular incident to a comma-separated value text file.</td>
</tr>
<tr>
<td>URL</td>
<td>Description</td>
</tr>
<tr>
<td>-----</td>
<td>-------------</td>
</tr>
<tr>
<td><code>https://&lt;instance name&gt;.service-now.com/incident_list.do?CSV&amp;sysparm_orderby=sys_id</code></td>
<td>Export all incidents to a comma-separated value text file and sort the list by sys_id.</td>
</tr>
</tbody>
</table>

**Note:** ServiceNow enforces basic authentication for direct URL access. The data extracted from the URL contains only the fields to which the currently authenticated user has read access.
Call URL export programmatically
You can dynamically export data from a script or web service by calling a URL export from any programming language.

The following procedure includes code samples that demonstrate calling a URL export in C# for a .Net framework call:

1. Add the following Imports:

   ```csharp
   using System.Net;
   using System.IO;
   ```

2. Call the Download method:

   ```csharp
   static void Main(string[] args)
   {
       // Call to DownloadFile method supplying the URL and location to
       // save CSV file locally
       int read = DownloadFile("https://
       <instance>.service-now.com/incident_list.do?
       CSV&sysparm_query=priority=1&sysparm_orderby=assigned_to",
       "c:\\test\\incident.csv");
   }
   ```

3. Create a Download method as follows:

   ```csharp
   public static int DownloadFile(String url,
       String localFilename)
   {
       // Function will return the number of bytes processed
       // to the caller. Initialize to 0 here.
       int bytesProcessed = 0;
       // Assign values to these objects here so that they can
       // be referenced in the finally block
       Stream remoteStream = null;
       Stream localStream = null;
       WebResponse response = null;
       // Use a try/catch/finally block as both the WebRequest and
       Stream
       // classes throw exceptions upon error
       try
       {
           // Create a request for the specified remote file name
           WebRequest request = WebRequest.Create(url);
           // Create the credentials required for Basic Authentication
           System.Net.ICredentials cred = new
           System.Net.NetworkCredential("user_name", "password");
           // Add the credentials to the request
           request.Credentials = cred;
           if (request != null)
           {
               // Send the request to the server and retrieve the
               // WebResponse object
               response = request.GetResponse();
               if (response != null)
               {
                   // Once the WebResponse object has been retrieved,
                   // get the stream object associated with the
                   response's data
                   remoteStream = response.GetResponseStream();
                   // Create the local file
                   localStream = File.Create(localFilename);
               }
           }
       }
   }
   ```
// Allocate a 1k buffer
byte[] buffer = new byte[1024];
int bytesRead;
// Simple do/while loop to read from stream until
// no bytes are returned
do {
   // Read data (up to 1k) from the stream
   bytesRead = remoteStream.Read(buffer, 0, buffer.Length);
   // Write the data to the local file
   localStream.Write(buffer, 0, bytesRead);
   // Increment total bytes processed
   bytesProcessed += bytesRead;
} while (bytesRead > 0);
}
}
catch (Exception e)
{
    Console.WriteLine(e.Message);
}
finally
{
   // Close the response and streams objects here
   // to make sure they're closed even if an exception
   // is thrown at some point
   if (response != null) response.Close();
   if (remoteStream != null) remoteStream.Close();
   if (localStream != null) localStream.Close();
}
// Return total bytes processed to caller.
return bytesProcessed;

Break up a large export

If the number of records to be exported exceeds the actual export limit, you may want to break the export into smaller increments that do not place a significant performance load on the platform.

1. Filter the list to display the records you want to export.
2. Write down the number of records returned.
3. If the record number is higher than the defined threshold, issue a sysparm query for the first 10,000 records using the following syntax:

   https://<instance name>.service-now.com/syslog_list.do?
   XML&sysparm_orderby=sys_id&sysparm_record_count=10000

   This exports the first 10,000 records in order, sorted by the sys_id number.

4. Find the next record in order, such as 10,001.
5. Right-click the row and copy the sys_id of the next record you want to export.
6. Access the next series of records with a **greater than or equal to** query run against the **sys_id** of record 10,001.

The following example shows a query that uses a sys_id of b4aeb520a0a0b1001af10e278657d27. Use the syntax shown in this query to export the next set of records.

```xml
https://<instance name>.service-now.com/syslog_list.do?XML&sysparm_query=sys_id%3E%3Db4aeb520a0a0b1001af10e278657d27&sysparm_orderby=sys_id&sysparm_record_count=10000
```

**Note:** URL queries use typical percent encoding. In this example, the greater than sign (> ) is encoded as %3E and the equal sign (=) is encoded as %3D.

7. Continue issuing this query, using the starting sys_id for the next set of records until you have exported all the necessary records.

**Enable export debug logging**

When the property **glide.export.debug** is true, the instance logs export processing including database query time and the time taken to write data to the file.

When the property **glide.export.debug** is **true**, the instance logs export processing including database query time and the time taken to write data to the file. Debug logs are indicated by the text **Export API**. Prolonged use of this property can affect performance, so it is best to use it while debugging export processing, and then set the property back to **false**.

```plaintext
7/17/14 15:53:48 (500) EB39A310EB022100C46AC2EEF106FED9 Maximum record count for this instance is: 10000: , request is for: 0 Cap the Record count to Maximum Record Count
07/17/14 15:53:48 (522) EB39A310EB022100C46AC2EEF106FED9 Export API - ExportProcessor : Processing EXCEL export request, ExportParameters:TableName=incident, Query=active=true, Limit=10000, SortBy=null
07/17/14 15:53:48 (527) EB39A310EB022100C46AC2EEF106FED9 Export API - ExportProcessor : Export using background thread
07/17/14 15:53:48 (528) EB39A310EB022100C46AC2EEF106FED9 #748 / poll_processor.do -- total transaction time: 0:00:03.357, total wait time: 0:00:00.000, session wait: 0:00:00.000, semaphore wait: 0:00:00.000, source: 0:0:0:0:0:0:0:1%
07/17/14 15:53:48 (550) SYSTEM Enabling elevated role: security_admin
07/17/14 15:53:48 (588) SYSTEM Export API - ExcelExporter : 29 rows retrieved from database duration_milliseconds=2
07/17/14 15:53:49 (534) NONE New transaction
EB39A310EB022100C46AC2EEF106FED9 #751 /poll_processor.do
07/17/14 15:53:49 (544) EB39A310EB022100C46AC2EEF106FED9 #751 / poll_processor.do Parameters -------------------------
  sys_action=poll
  sysparm_processor=poll_processor
  job_id=a61a2314eb022100c46ac2eeef106fe0a
07/17/14 15:53:49 (547) EB39A310EB022100C46AC2EEF106FED9 #751 / poll_processor.do -- total transaction time: 0:00:00.013, total wait time: 0:00:00.000, session wait: 0:00:00.000, semaphore wait: 0:00:00.000, source: 0:0:0:0:0:0:0:1%
07/17/14 15:53:49 (740) SYSTEM Export API - ExcelExporter : Rows written to file duration_milliseconds=1150
```
**Import an XML file**

After you have successfully exported data from the source instance, you can import the XML file directly to the target instance.

Role required: admin

Importing XML does not trigger business rules or update the instance cache.

1. Sign in to the target instance (the instance that should receive the data).
2. In the banner frame, click the Elevate privileges icon (𝐸) beside the user name.
3. In the Activate an Elevated Privilege dialog box, select the **security_admin** check box and click OK.
4. Navigate to any list in the system.
   Any list can be used because the XML file contains the destination table name for the records.
5. Perform the appropriate action for the list version.

<table>
<thead>
<tr>
<th>Version</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>List v2</td>
<td>Open any column context menu and select <strong>Import XML</strong>.</td>
</tr>
<tr>
<td>List v3</td>
<td>Open the list title menu and select <strong>Import XML</strong>.</td>
</tr>
</tbody>
</table>
6. In the import screen, click **Choose File** and select the previously exported XML file.

![Importing records from an XML file will not run Business Rules](Image)

(1) Choose file to upload:

| Choose File | No file chosen |

(2) Upload the file

![Upload](Image)

7. Click **Upload**.

![Note: If the data does not import, navigate to System Definition > Tables & Columns and verify that the table from which the data was exported also exists in the instance importing the data. If the table does not exist in that instance, you can move it using an update set.](Image)

**Export sets**

Export sets allow you to push data from an instance to an external file.

You can export data to a remote system using a MID Server.

![Note: You must use a MID Server from the Geneva release or later. Earlier MID Server releases do not support export sets. Export sets are not supported on MID Servers in a cluster.](Image)

**Create an export set**

Create an export set to export records from your instance to a file on a MID Server.

Role required: export_set_admin

![Note: Export sets do not export attachments to records. To download an attachment, either use the REST Attachment API (HTTP request originates from a third-party HTTP client), or use the outbound REST Message module to send the attachment from the instance (HTTP request originates from the instance).](Image)

1. Navigate to **System Export Sets > Create Export Set**.
2. Enter a descriptive **Name** for the export set.
3. In the **What to export** section, define what data to export in one of these ways.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Yes and select an Export Definition record.</td>
<td>Use this configuration if you have already created an export definition record specifying what data to export.</td>
</tr>
</tbody>
</table>
4. In the **Where to export to** section, define where you want to export data to in one of these ways.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Yes and select an Export Target record.</td>
<td>Use this configuration if you have already created an export target record specifying where to export data to.</td>
</tr>
<tr>
<td>Select No and select a MID Server, and specify a path on the MID Server to save the exported data to.</td>
<td>Use this configuration if you have not created an export target record. A new export target record is created automatically for the selected MID Server and file path. You can modify the export target record as needed after creating the export set.</td>
</tr>
</tbody>
</table>

5. Click **Submit**.

After creating the export set, the Export Set form appears. You can configure advanced options from the form such as specifying a data format or scheduling recurring exports.

**Export Set form fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a descriptive name for this export set.</td>
</tr>
<tr>
<td>File name</td>
<td>Enter a name for the target file.</td>
</tr>
<tr>
<td>Format</td>
<td>Select the format of the target file, such as CSV.</td>
</tr>
<tr>
<td>Append timestamp</td>
<td>Select this check box to append the current date and time to the name of the exported file.</td>
</tr>
<tr>
<td>Export definition</td>
<td>Select the export definition that specifies the data to export.</td>
</tr>
<tr>
<td>Export target</td>
<td>Select the export target that specifies the location you want to export to.</td>
</tr>
</tbody>
</table>

**Create an export set from a list**

You can quickly create an export set from a list.

Role required: export_set_admin

1. Navigate to a list of records.
2. Perform the appropriate action for the list version.

<table>
<thead>
<tr>
<th>Version</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>List v2</td>
<td>Right-click the list header and select Export &gt; Export Set.</td>
</tr>
<tr>
<td>List v3</td>
<td>Open the list title menu and click Export, and then click Export Set.</td>
</tr>
</tbody>
</table>

The Export Set form appears. An export definition is created automatically based on the list.

3. Configure the export set as needed.
4. Click **Submit**.
Create an export definition

Create an export definition to define what data to export in an export set.

Role required: export_set_admin

An export definition specifies the data to be exported in an export set. This data includes a table, one or more fields, and optionally a filter to limit the included records.

1. Navigate to System Export Sets > Export Definition.
2. Click New.
3. Enter a descriptive Name for the export definition.
4. Select the Table to export data from.
5. Select one or more Fields from the selected table to export data from.
6. Optional: Specify a Filter to export only certain records from the selected table.

Specifying a filter condition on the Created (sys_created_on) or Updated (sys_updated_on) fields may prevent scheduled data exports from using delta exports functionality. Do not specify filter conditions on these fields if you intend to use scheduled delta exports.

Create an export target

Define where to export data to by creating an export target.

Role required: export_set_admin

You must use a MID server as the export destination.

Navigate to System Export Sets > Export Targets and create a new record (see table for field descriptions).

Export target fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a descriptive name for the export target.</td>
</tr>
<tr>
<td>MID Server</td>
<td>Select the MID Server to export to. The MID Server must have a Validated value of Yes and a Status value of Up.</td>
</tr>
</tbody>
</table>

**Note:** You must use a MID Server from the Geneva release or later. Earlier MID Server releases do not support export sets. Export sets are not supported on MID Servers in a cluster.

File Path | Specify a path relative to the MID Server directory to save the exported data to. The user account used to run the MID Server must have permission to write to this location.
Export set supported file types

Export sets support multiple file types for exporting and pushing data.

File types

You can export to these formats:

- CSV
- XML
- Excel
- JSON

Schedule an export

You can schedule an export to regularly push data from an export set to a remote destination. By setting up a recurring, scheduled export you are able to regularly push data to an external location, such as for reporting or for preserving a snapshot of the data.

Role required: export_set_scheduler or export_set_admin

You can configure scheduled export sets to export only new or changed records using delta exports.

1. Navigate to **System Export Sets > Scheduled Exports**.
2. Click **New**.
3. Fill in the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a descriptive name for this scheduled export.</td>
</tr>
<tr>
<td>Export set</td>
<td>Select the export set to schedule.</td>
</tr>
<tr>
<td>Run as</td>
<td>Select the user to run the scheduled export as. Ensure the user has any roles needed to view the data to export.</td>
</tr>
<tr>
<td>Run</td>
<td>Select the frequency for scheduled export.</td>
</tr>
<tr>
<td>Day</td>
<td>Select which day of the week or month to run this scheduled export.</td>
</tr>
<tr>
<td>Repeat interval</td>
<td>Enter the number of days and hours to wait before repeating this scheduled export.</td>
</tr>
<tr>
<td>Time</td>
<td>Enter the time of day to run the scheduled export.</td>
</tr>
<tr>
<td>Delta Exports</td>
<td>Select this check box to enable delta functionality for this scheduled export. When selected, only new or changed records are exported.</td>
</tr>
</tbody>
</table>
Field | Description
--- | ---
Delta on or after | Select **Updated** to export all records that changed since the last export, including new records. Select **Created** to export only new records created after the last export.

**Note:** If the export definition already includes a filter condition on the sys_updated_on or sys_created_on fields, enabling delta exports will prevent you from saving the scheduled data export record. An error appears at the top of the form in this event.

Last export scheduled run | Leave this field blank to export all records from the export definition. When using delta exports, this field is set automatically each time the scheduled export runs. Records updated or created after this date and time are included in the export delta, depending on the Delta on or after value.

Scripts

Conditional | Select this check box to run the schedule only when a condition is met.
Condition | Write the script to be used to evaluate whether the export should run. This field is visible if you select the Conditional check box.

Execute pre-export script | Select this check box to run a script before the export begins.
Pre script | Write the script you want to run before the data is exported. This field is visible if you selected the Execute pre-export script check box.

Execute post-export script | Select this check box to run a script after the export finishes.
Post script | Write the script you want to run after the export finishes. This field is visible if you selected the Execute post-export script check box.

4. Click **Submit**.

You can click the **Execute Now** button to run the export immediately and confirm the data is exported as expected.

**Scheduled export set delta exports**

Delta exports include only the records that changed since the last scheduled export.

You can use delta export for regular tables only, such as the task and problem tables.

**Important:** You cannot use delta export for a database view table, which is a virtual table that joins physical tables.

A database view does not include system fields such as sys_created_on, sys_created_by and sys_updated_on. Because the system date fields are not included in the database view, you cannot use delta exports with database views since there is no way to know when the table was last updated.
Scheduled export set scripting options

When scheduling an export set, you can access certain JavaScript objects. Use these objects in scheduled export set scripts, such as the **Pre-script** and **Post-script** fields.

**cancel**

Set this object to `true` to stop the export action. Any child export sets are also cancelled if the parent is cancelled. This object is available only in the **Pre-script** field.

**Example:** Use the **Pre-script** field to evaluate the conditions of the export and determine whether to cancel the export process. To cancel the export process, use the following call:

```javascript
cancel = true;
```

**export_set**

Get the GlideRecord object for the new export set. This variable allows you to query the following columns from the `sys_export_set` table:

- name
- `sys_id`
- state
- `table_name`

This object is available in both the **Pre-script** and **Post-script** fields.

**Example:** If you want to use information from the export set, you can specify one of the properties of the `export_set` variable.

```javascript
var x = export_set.sys_id;
```

Export set history

An export set history record is automatically created whenever an export set runs, either scheduled or manually started by a user. Export set history records allow you to monitor and troubleshoot the progress of export sets.

Fields on the Export History form display the current status of the export set. The **Export Log** related list shows a detailed list of changes to the export set status.

**Export History form fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export set</td>
<td>The export set that was run.</td>
</tr>
<tr>
<td>Started</td>
<td>The date and time the export started.</td>
</tr>
<tr>
<td>Completed</td>
<td>The date and time the export completed.</td>
</tr>
<tr>
<td>Export time</td>
<td>The amount of time it took to export the data, excluding the</td>
</tr>
<tr>
<td></td>
<td>time it took to transfer the data to the target.</td>
</tr>
<tr>
<td>Run time</td>
<td>The amount of time it took to export the data, including the</td>
</tr>
<tr>
<td></td>
<td>time it took to transfer the data to the target.</td>
</tr>
<tr>
<td>State</td>
<td>The current state of the export.</td>
</tr>
</tbody>
</table>
### ServiceNow, DocVersion, Now Platform administration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delta export</td>
<td>The export used delta export functionality if this check box is selected.</td>
</tr>
<tr>
<td>ECC queue</td>
<td>The ECC Queue record associated with this export set run. This field is visible only to users with the admin role.</td>
</tr>
<tr>
<td>MID Server Attachment</td>
<td>A MID Server attachment record containing a copy of the exported file. The exported file is attached to this record in addition to being saved on the MID Server.</td>
</tr>
</tbody>
</table>

The **State** field may have the following values.

#### States

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exporting</td>
<td>The export set is creating a file with the data to export.</td>
</tr>
<tr>
<td>MID Server Processing</td>
<td>The export set successfully created a file with the data to export. The file is being processed by the MID Server.</td>
</tr>
<tr>
<td>Completed</td>
<td>The export set successfully ran and sent the exported file to the target.</td>
</tr>
<tr>
<td>Completed wth errors</td>
<td>The export set ran, but encountered one or more errors.</td>
</tr>
<tr>
<td>Cancel requested</td>
<td>A user requested that the export set be cancelled.</td>
</tr>
<tr>
<td>Cancelled</td>
<td>The export set was cancelled.</td>
</tr>
</tbody>
</table>

### Cancel an export set

You can cancel a running export set to stop the data from being sent to a MID server.

Role required: export_set_admin

You can cancel only exports that have not yet been sent to a MID server. You cannot cancel an export after it reaches the **MID Server Processing** state.

1. Navigate to **System Export Sets > Export Sets**.
2. Select an export set.
3. In the **Export Histories** related list, select a record with the **State** value of **Exporting**.
4. Click **Cancel Export Set**.

### Export Set properties

These properties control the behavior of export sets.

#### Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.scheduled_export.stop_on_parent_error</td>
<td>When true, if a parent scheduled export set encounters an error, scheduled child export sets do not run. This property is false by default.</td>
</tr>
</tbody>
</table>
Import sets

Import sets allow administrators to import data from various data sources, and then map that data into ServiceNow tables.

Explore
- Upgrade to.
- Import sets key concepts

Set up
- Create a data source
- Create a transform map

Use
- Run an import
- Importing Data into ServiceNow
- Schedule a data import
- Easy import

Administer
- Import sets properties
- Troubleshoot import set performance

Develop
- Developer training
- Developer documentation
- Field map script variables
- Scheduled data import scripting options

Integrate
- Web service import sets
- Importing from another ServiceNow instance
- Apply CI Identification and Reconciliation to Import Sets

Troubleshoot and get help
- Blog: Troubleshooting missing data in date fields
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

Import sets key concepts

Learn about Import Sets before importing data to your instance.

The Import Sets table acts as a staging area for records imported from a data source.

Note: You should not import data in extremely large chunks. Creating an extremely large import set can cause delays and system outages.

A transform map determines the relationships between fields displaying in an Import Set table and fields in an existing ServiceNow table, such as the Incidents or Users table.

Importing sets skip records when the data in the instance matches the data being imported.

Note: Import Sets run as user System and therefore cannot add data to encrypted fields.

Terminology

Key terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import Set table</td>
<td>A table that acts as a staging location for records imported from a data source before transforming those records. Fields on these tables are generated automatically based on imported data and should not be modified manually.</td>
</tr>
</tbody>
</table>
## Term

<table>
<thead>
<tr>
<th>Data source</th>
<th>A record that defines where to get the data to import. A data source may point to a file, a JDBC-compatible database, or an LDAP organizational unit.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transformation</td>
<td>The conversion of data from an import set table to another table according to the rules defined in a transform map.</td>
</tr>
<tr>
<td>Transform map</td>
<td>A set of field maps that define the relationships between fields in an import set and fields on a table, such as Incident. During transformation, data is copied from the Import Set table to the destination table based on the transform map. A single import set field may be mapped to multiple fields on other tables.</td>
</tr>
<tr>
<td>Robust import set transformer</td>
<td></td>
</tr>
<tr>
<td>Foreign record insert</td>
<td>A foreign record insert occurs when an import makes a change to a table that is not the target table for that import. This happens when updating a reference field on a table. For example, when updating a value for the caller on an incident, the import is actually updating the sys_user table.</td>
</tr>
<tr>
<td>Coalesce</td>
<td>Lets you update existing target table records when transforming import data. You can specify whether a <strong>Target field</strong> should be used to coalesce on when import set records are transformed. If the field map <strong>Coalesce</strong> check box is selected, when the import set row is transformed, the instance checks for an existing record in the target table that has the same value in the <strong>Target field</strong> as the import set row <strong>Source field</strong>. If an existing record with a matching value in the target table is found, that record is updated. If no matching record is found, then a new record is created in the target table.</td>
</tr>
</tbody>
</table>

## Supported import formats

You can import data from several different file formats or external data sources.

### File formats

<table>
<thead>
<tr>
<th>Format</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSV</td>
<td>CSV files must comply with the proposed CSV standard in <a href="https://tools.ietf.org/html/rfc4180">RFC4180</a>. In particular, this means that double quotes may not appear inside fields. The first row of data in an imported CSV file becomes the header row and defines the columns for that import set.</td>
</tr>
<tr>
<td>Excel</td>
<td>Excel files must have the XLS or XLSX extension.</td>
</tr>
<tr>
<td>XML</td>
<td>XML files must have a consistent XPath for each data row.</td>
</tr>
</tbody>
</table>
ServiceNow can import data from the following external data sources.

### External data sources

<table>
<thead>
<tr>
<th>Data Source</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>JDBC</td>
<td>JDBC imports require a valid transform map. Some network configurations may require a MID Server.</td>
</tr>
<tr>
<td>LDAP</td>
<td>LDAP imports require a valid transform map.</td>
</tr>
<tr>
<td>OIDC</td>
<td>OIDC imports require a valid transform map.</td>
</tr>
<tr>
<td>REST (IntegrationHub)</td>
<td>REST imports require a valid transform map.</td>
</tr>
<tr>
<td>Custom (Load by Script)</td>
<td>Custom imports require a valid transform map.</td>
</tr>
</tbody>
</table>

### Transform maps versus robust import set transformers

Both transform maps and robust import set transformers convert data. Transform maps convert data from the staging table to the destination file. Robust import set transformers convert data from a source table to a message listener. If a data source has both a transform map and a robust import set transformer, the system uses the robust import set transformer instead of the transform map.

### Import set scheduled cleanup

The Import Set Deleter scheduled job cleans up old import set data every day at midnight. By default, the job deletes all import sets that are older than 7 days, as well as the associated import set table records. If this scheduled job is not active on your instance, activate it to mitigate the growing import set tables you may have, especially when using recurring imports.

**Note:** If scheduled cleanup is not currently active on your system, you must ensure that your import set tables are not too big (> 5 million records total across all tables) before enabling this cleanup. If the tables are too big, manually delete the records first before proceeding. Please contact Customer Service and Support to coordinate the deletion of this data.
For procedures, see Delete import sets.

**Import set table deleter**

You can manually delete any or all of the following import set tables:

- Computer
- User
- Notification
- Location

You can also delete the related transform maps, or you can delete data only and preserve the table structure.

For procedures, see Delete import set tables.
Concurrent imports

Split incoming data into multiple import sets and transform the import sets concurrently to reduce processing time.

Running a concurrent import can be helpful when order does not matter and imports take a long time due to large data sets with time-consuming scripts. If order matters, you can split the import into multiple partitions to ensure that each partition is processed in order.

**Note:** Concurrent imports add processing and monitoring overhead. Use them only with large data sets.

Enable concurrent imports only after fine-tuning all other parameters, such as database indexes and transformations.

Scheduling concurrent imports

You enable concurrent imports by selecting **Concurrent Import** on the Scheduled Data Import form. For instructions, see Schedule a data import.

When the schedule runs a concurrent import, the system pulls the data from databases, Excel spreadsheets, CSV files, or other sources to a temporary staging table, and then transforms the data from the staging table to the target table.

When you run a concurrent import, the system creates multiple import sets, up to the value of the `glide.scheduled_import.max.concurrent.import_sets` system property (default = 10). For example, a two-node cluster produces four import sets, and a ten-node cluster produces ten import sets.

Import Set Transformer job

Each active node runs two Import Set Transformer jobs every minute, and those jobs poll the Concurrent Import Sets Jobs queue, pick import sets from the queue, and transform those import sets. All jobs run concurrently, depending on the availability of worker threads.

Concurrent Import Set record

Each concurrent import creates a Concurrent Import Set record. The form view shows all related import sets, concurrent import set jobs, and transform histories.

You can resume or reprocess any import set. For more information, see Monitor concurrent import sets.

Concurrent Import Sets Jobs queue

After loading data, the system adds the import sets to the Concurrent Import Sets Jobs table. The Concurrent Import Sets Jobs table indicates the job type and status of each concurrent import set job.

For more information, see Monitor concurrent import set jobs.

Partitioning concurrent imports

You can partition import sets to maintain the processing order within each partition.

By default, the system allocates records to import sets in a round robin fashion. However, you can write a custom script to define a custom `partition key` that identifies the target import set. Every row with the same partition key adds to the same import set, and the data in that import set is processed in sequential order.
Hierarchical imports

You can create a scheduled import set hierarchy by scheduling an import to run after another import set completes. One parent scheduled import can have many child scheduled imports, and each child scheduled import executes in the order specified. For concurrent scheduled imports, child scheduled imports can be started only after all Import Set Transformer jobs complete.

The last Import Set Transformer job starts the next import in the hierarchy.

The system generates an execution plan at the beginning of parent import process. Each import process uses the execution plan to fetch the next process to invoke. For concurrent imports, the last Import Set Transformer job fetches the next import and executes it.

Synchronized inserts

Coalesce fields help define uniqueness among records. The transformation process checks for an existing record with the coalesce values and updates the existing record, if it exists, or inserts a new record if none exists. For more information, see Updating records using coalesce.

By default, concurrent imports allow each running import set to insert new records. When an import set inserts a record, it establishes a write lock on the target table to prevent other import sets from inserting the same record.

Tables for concurrent imports

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concurrent Import Set (sys_concurrent_import_set)</td>
<td>Stores details of each concurrent import set in import set records.</td>
</tr>
<tr>
<td>Concurrent Import Set Jobs (sys_concurrent_import_set_job)</td>
<td>Lists the import sets to be processed.</td>
</tr>
<tr>
<td>Execution Context for Scheduled import (sys_execution_context)</td>
<td>Specifies the execution context for each scheduled import. The execution context specifies the next scheduled import to use when processing a hierarchical scheduled import.</td>
</tr>
<tr>
<td>Hierarchical scheduled import execution plan (sys_execution_plan)</td>
<td>Stores the execution plan for hierarchical imports. The execution plan is a tree structure that identifies which scheduled import runs after the preceding scheduled input.</td>
</tr>
</tbody>
</table>

Domain Separation with concurrent imports

You can add the sys_domain field to a scheduled import table to enable domain separation for the import set. Both import set loading and transform jobs run in the domain specified in the scheduled import set job.
Data sources

Data sources are used to create an import set so that data can be processed, if necessary, prior to being mapped onto a production table.

### Data Source Types

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File</td>
<td>Data is in a recognized file format, accessible locally or remotely through several file retrieval methods.</td>
</tr>
<tr>
<td>JDBC</td>
<td>Data is in a database, accessible using JDBC. Customer Service and Support supports Oracle, MySQL, Sybase, DB2 Universal, and MS SQL Server drivers.</td>
</tr>
<tr>
<td>LDAP</td>
<td>Data is in an LDAP server, accessible through the LDAP or LDAPS ports, 389 and 636 respectively.</td>
</tr>
<tr>
<td>OIDC</td>
<td>Data is accessible via OIDC.</td>
</tr>
<tr>
<td>REST (IntegrationHub)</td>
<td>Data is in a REST API, accessible through IntegrationHub.</td>
</tr>
<tr>
<td>Data Stream IntegrationHub</td>
<td>Data is loaded from a Data Stream Action, accessible through IntegrationHub.</td>
</tr>
<tr>
<td>Custom (Load by Script)</td>
<td>Data is obtained using a custom script.</td>
</tr>
</tbody>
</table>

### File type data sources

Import a file from a local source, a remote network server, or another instance by providing a path and authentication information.

For file type import sets, you can select from a list of file retrieval methods: SFTP, FTP, FTPS, HTTP, HTTPS, and SCP.

**Note:** FTPS is not recommended because it is no longer supported by some firewall vendors. Consider using SFTP as an alternative.

### File retrieval methods

The following file retrieval methods are available to copy the file from where it resides to ServiceNow to be loaded into an import set.

After defining the files that are compatible for importing, define how the files can be imported.

**Note:** For the import to succeed, your FTP server and client must be set up for the same authentication mechanism that you select here.

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attachment</td>
<td>Attach a file to the record and import that file in an import set.</td>
</tr>
<tr>
<td>SFTP</td>
<td>Retrieve a file using SFTP. Fields are provided for the server name and login credentials.</td>
</tr>
<tr>
<td>Method</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>FTP</td>
<td>Retrieve a file from an FTP server in your network. Fields are provided for the server name and login credentials. <strong>Note:</strong> FTP transfers are sent as clear text and cannot be encrypted. Use SCP or SFTP instead whenever possible.</td>
</tr>
<tr>
<td>FTPS (Auth SSL) [not recommended]</td>
<td>Not recommended because FTPS is no longer supported by some firewall vendors. Consider using SFTP as an alternative. An FTP Secure authentication command issued through the Secure Socket Layer (SSL) protocol. This method is also known as explicit FTP over SSL.</td>
</tr>
<tr>
<td>FTPS (Auth TLS) [not recommended]</td>
<td>Not recommended because FTPS is no longer supported by some firewall vendors. Consider using SFTP as an alternative. An FTP Secure authentication command issued through the Transport Layer Security (TLS) protocol. This method is also known as explicit FTP over TLS.</td>
</tr>
<tr>
<td>FTPS (Implicit SSL) [not recommended]</td>
<td>Not recommended because FTPS is no longer supported by some firewall vendors. Consider using SFTP as an alternative. In implicit security, the FTPS server defines a specific port for the client (990) to use for secure connections. Implicit security automatically begins with an SSL connection the moment an FTPS client connects to an FTPS server.</td>
</tr>
<tr>
<td>FTPS (Implicit TLS) [not recommended]</td>
<td>Not recommended because FTPS is no longer supported by some firewall vendors. Consider using SFTP as an alternative. In implicit security, the FTPS server defines a specific port for the client (990) to use for secure connections. Implicit security automatically begins with a TLS connection the moment an FTP client connects to an FTP server.</td>
</tr>
<tr>
<td>HTTP</td>
<td>Retrieve a file using HTTP. Fields are provided for the server name and login credentials. <strong>Important:</strong> For HTTP and HTTPS protocols, the file path is automatically URL encoded. Do not specify a URL-encoded file path when using either of these protocols.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Retrieve a file using HTTPS. Fields are provided for the server name and login credentials. Use this method to transfer data between ServiceNow instances.</td>
</tr>
</tbody>
</table>
### File data source examples

These examples describe how to import various file types as data sources.

#### Excel data source file

You can import using both the XLSX format and the legacy XLS format. XLS is the default format for spreadsheets created in Excel for versions 2003 and older. XLSX is the default format for Excel 2007 or later. Use XLSX instead of legacy XLS whenever possible for optimal performance.

**Note:** All .xls files must use the 1900 date system as opposed to the 1904 date system. The 1904 date system causes your dates to be imported with a year that is four years earlier than what appears in your spreadsheet. Refer to MS Support for additional information about date systems.

---

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCP</td>
<td>The Secure Copy protocol (SCP) securely transfers files between a local and a remote host or between two remote hosts, using the Secure Shell (SSH) protocol.</td>
</tr>
</tbody>
</table>
XML data source file

XPath for each row

XML data source definitions have an extra field to specify the XPath for each row. This field is an XPath expression to select the elements whose children are converted to rows in the import set table. Each selected element causes a row to be created in the import set table. The children of the selected element are converted into columns in the row. For example, to import the asset information from the sample XML file below, the XPath expression should be specified as /export/asset. This expression matches the three <asset> elements in the file, so three rows are created. Although you could also specify //asset, this expression is much less efficient for large files. Use the absolute location path form for XPath expressions when using the XML loader. In other words, avoid expressions containing // unless strictly necessary.

Be careful not to specify an insufficiently restrictive XPath expression with a large XML file. For example, the expression /export would be wrong for the following sample file, since it matches the document (root) element. In general, you should never specify an XPath expression which matches the root element unless you want everything in the document to be made into a single row. Specifying an insufficiently restrictive XPath expression when attempting to load large XML files could result in lengthy processing times and incorrect output. For this reason, it is best to test and debug XML data source specifications with small XML files containing only a few rows worth of data. Once the specification has been tested, you can run it again with the full file.

(userInfo) elements

Note that the <userInfo> elements contained within <asset> contain child elements. This type of nesting creates a column called userInfo that contains XML for the <userInfo> element. If Expand child nodes is checked, individual columns are also created for userInfo/lastName and userInfo/firstName. If Expand child nodes is not checked, only the userInfo XML column is created.

<?xml version= "1.0" encoding= "utf-8"?><export><asset><assetTag>AT-01939</assetTag><type>Desktop</type><os>Windows 7 Professional</os><lastlogondate>12-07-2010 12:31:24</lastlogondate><userInfo><lastName>Loo</lastName><firstName>David</firstName></userInfo><isenabled>true</isenabled></asset><asset><assetTag>AT-53480</assetTag><type>Desktop</type><os>Windows 7 Professional</os><lastlogondate>09-07-2010 13:25:53</lastlogondate><userInfo><lastName>Merritt</lastName><firstName>Norris</firstName></userInfo><isenabled>true</isenabled></asset><asset><assetTag>AT-55782</assetTag><type>Desktop</type><os>Unknown</os><lastlogondate>01-01-1900 00:00:00</lastlogondate><userInfo><lastName>Currie</lastName><firstName>Mike</firstName></userInfo><isenabled>true</isenabled></asset></export>

Loading data from an XML file

When loading data from an XML file, ServiceNow samples the first 10 records to determine what fields are required to hold the data. If none of the first 10 records specify a value for a field, ServiceNow does not add that field to the table that holds the imported data. Ensure that at least one of the first 10 records specifies a value for any fields being imported.

If the XML file used for an XML data source does not contain a field in the first 10 nodes, the field is ignored. To import the field and ensure it is not ignored, you can add the glide.db.impex.XMLLoader.max.scan_nodes system property with a value greater than or equal to the position of the node where the field is first encountered. This property applies to all XML data sources. glide.db.impex.XMLLoader.max.scan_nodes defaults to 10, but you can enter a value from 1 to 2147483647 to specify how many nodes should be scanned to determine the values to be used for the import. You can specify -1 to scan all nodes in the XML files.
Important: If you specify -1 or increase the value of glide.db.impex.XMLLoader.max.scan_nodes beyond the default of 10, all XML import processing may incur a significant increase in overall load time.

CSV data source file

CSV files are used as a cross-compatible file format for transferring files across platforms. A CSV file is a text file that defines a grid, where commas define columns and line breaks define rows. To define precise spacing for importing strings, you can optionally wrap text in quotes.

"user_name","name","email","sys_created_on","active"
"jared.laethem","Jared Laethem","jared.laethem@yourcompany.com","2008-02-24 22:21:32","true"
"jerrod.bennett","Jerrod Bennett","jerrod.bennett@yourcompany.com","2007-08-12 12:12:18","true"
"eric.schroeder","Eric Schroeder","eric.schroeder@yourcompany.com","2007-07-03 11:50:20","true"
"rob.woodbyrne","Rob Woodbyrne","rob.woodbyrne@yourcompany.com","2007-07-03 11:49:57","true"
"admin","System Administrator","admin@yourcompany.com","2007-07-03 11:48:47","true"
"christen.mitchell","Christen Mitchell","christen.mitchell@yourcompany.com","2007-05-16 15:26:42","true"
"rob.phillips","Rob Phillips","rob.phillips@yourcompany.com","2007-01-22 11:25:34","true"
"davin.czukowski","Davin Czukowski","davin.czukowski@yourcompany.com","2006-07-11 14:01:26","true"
"luke.wilson","Luke Wilson","luke.wilson@yourcompany.com","2006-02-07 15:29:48","true"
"bow.ruggeri","Bow Ruggeri","bow.ruggeri@yourcompany.com","2005-07-07 11:39:58","true"
"don.goodliffe","Don Goodliffe","don.goodliffe@yourcompany.com","2005-05-02 12:28:40","true"
"david.loo","David Loo","david.loo@yourcompany.com","2005-02-22 16:00:00","true"
"guest","Guest","guest@yourcompany.com","2004-05-01 17:00:00","true"
"f red.luddy","Fred Luddy","fred.luddy@yourcompany.com","2004-05-01 17:00:00","true"

When using CSV files, you can specify the encoding charset using the Properties field on the Data Source form. You may need to configure the Data Source form to see this field. For example, to use utf-8 encoding, enter charset=utf-8.

Data in single column

For the JSON and XML formats, this feature lets you store a full record in a single column.

The column name used to store the full record is data.

If you create a JSON format data source to save data in a single column, selecting the Data in single column check box updates the following options:

- **Discard Array** becomes unselected and is removed from the form.
- **Expand node children** becomes selected and is removed from the form.
If you create an XML format data source to save data in a single column and you select the **Data in single column** check box, **Expand node children** becomes selected and is removed from the form.

### Custom (Parse by Script) format

When you select a **Type** of *File* and a **Format** of *Custom (Parse by Script)*, a Javascript editor called **Parsing script** appears. You can use the parsing script to create customized Javascript to parse input lines into the list of maps.

The Javascript has three predefined parameters:

- The **line** parameter is a string which contains line data from the source file.
- The **lineNumber** is the line number from the source file for this line data.
- The **result** parameter is used to pass back the parsed result from Javascript.
The **result** parameter is an instance of Java object ScopedScriptParseResult. When you type `result.`, four available methods appear as script auto-complete in the Javascript editor:

- `void setSkip(boolean skip);`
- `boolean getSkip();`
- `addRow(Map<String, String> map);`
- `List<Map<String, String>> getRows();`

The `setSkip()` and `getSkip()` set and retrieve the skip flag. When the skip flag is set to true, the entire parsing result from Javascript is ignored.

The `addRow()` adds one map of the parsing row result, which is inserted into the staging table.

The `getRows()` retrieves all rows of the current parsing result, which are inserted into the staging table.

One line of source data can contain one row or multiple rows. It is up to the script writer to decide how to process the line data. For example, for line data `name=john, computer=windows; name=joe, computer=linux; name=linda, computer=windows`, if you use a semicolon (`;`) as a row break, then this line contains three rows of data. Each row is a map with two keys: `name` and `computer`. The `name` and `computer` become the column names for the staging table schema. You could use the following sample of Javascript to parse this line data:

```javascript
(function(line, lineNumber, result) {
    var rowArr = line.split(";");
    var i;
    for(i in rowArr) {
        var map = {};
        var arr = rowArr[i].split","");
        var x;
        for(x in arr) {
            var items = arr[x].split("=");
            map[items[0]]=items[1];
        }
        result.addRow(map);
    }
})(line, lineNumber, result);
```

The script writer must add the result so that the result is inserted in the staging table.
Processing custom CSV files
You can process CSV files that are delimited by a character other than commas.

This is an advanced step to create a CSV import. Normally, you would upload the data and import it directly using System Import Sets, which will create this CSV data source for you automatically.

1. Create the data source record.
2. Attach the CSV file to the data source.
3. Customize the Data Source form and add the CSV Delimiter field.
4. Enter the character you want to use as the CSV file delimiter, such as the pipe symbol (|).
5. Test load the data source.

Importing JSON files
These examples demonstrate how to import various types of JSON data and the necessary path for each row. JSON files that you import should follow these guidelines.

• For JSON arrays, the path for each row must specify the array root element twice, such as /incidents/incidents.
• JSON files should follow RFC-4627. For example, a single comma should separate a value from the following name. Names within an object should be unique.
• Predicates such as @element, [index], or text(), as well as Axis such as children, siblings, or ancestors are not supported.

Simple array

• Path for each row: /incidents/incidents
• Result: 2 records

In this example, the path for each row includes the array root node /incidents twice. This is necessary when importing an array.

```json
{
    "source":"HI",
    "incidents": [
        {
            "number":"INC0000001",
            "short_description":"Can't read email"
        }
    ],
```
Array in 2nd level

- Path for each row: `/problems/data/data`
- Result: 4 records

In this example, the path for each row includes the array root node `/data` twice.

```json
{
  "problems":{
    "id":0,
    "data":[
      {
        "number":"PRBTEST001",
        "short_description":"testsd1"
      },
      {
        "number":"PRBTEST002",
        "short_description":"testsd2"
      },
      {
        "number":"PRBTEST003",
        "short_description":"testsd3"
      }
    ]
  }
}
```

Nested array

- Path for each row: `/problems/problems/data/data`
- Result: 3 records

In this example, the path for each row includes the root nodes for both arrays twice, `/problems` and `/data`.

```json
{
  "problems": [ 
    { 
      "id":0,
      "data": [ 
        { 
          "number":"PRBTEST001",
          "short_description":"testsd1"
        },
        { 
          "number":"PRBTEST002",
          "short_description":"testsd2"
        },
        { 
          "number":"PRBTEST003",
          "short_description":"testsd3"
        }
      ]
    }
  ]
}
```
Supporting child (nested) arrays

By default, import does not support child (nested) arrays. You can enable support by unchecking the **Discard Arrays** check box in the Data Source view. The following table describes different behaviors when enabling and disabling child array support.

```json
{
    "response":{
        "docs":[
            {
                "id":"id_val",
                "childrenArray":[1,2,3],
                "anotherArray":[{"key1":"value1"}, {"key1": "value2"}],
                "elementWithArray":{"childrenArray":[1,2,3]}
            }
        ]
    }
}
```

<table>
<thead>
<tr>
<th>Path</th>
<th>Discard Arrays Enabled</th>
<th>Discard Arrays Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>/response/docs/docs</td>
<td>Creates one record with the following columns and values:</td>
<td>Creates one record with the following columns and values:</td>
</tr>
<tr>
<td></td>
<td>- Id : id_val</td>
<td>- Id : id_val</td>
</tr>
<tr>
<td></td>
<td>- elementWithArray : {}</td>
<td>- childrenArray : [1, 2, 3]</td>
</tr>
<tr>
<td></td>
<td>Any arrays found in a record, such as childrenArray or anotherArray, are not created as columns in the import table.</td>
<td>anotherArray : [{&quot;key1&quot;: &quot;value1&quot;}, {&quot;key1&quot;: &quot;value2&quot;}]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- elementWithArray : {}</td>
</tr>
<tr>
<td>/response/docs/docs/anotherArray/anotherArray</td>
<td>Creates two records, each with one column: key1.</td>
<td>Creates two records, each with one column: key1.</td>
</tr>
<tr>
<td>/response/docs/docs/childrenArray/childrenArray</td>
<td>Does not work and returns a Path should always refer JSON Objects error because the values in the array are not in a key-value structure.</td>
<td>Does not work and returns a Path should always refer JSON Objects error because the values in the array are not in a key-value structure.</td>
</tr>
</tbody>
</table>
Orphan array

**Important:** This format is supported. A JSON array must always be inside an element. The JSON file must always start with `{` and end with `}`.

```
{
  "number":"PRBTEST001",
  "short_description":"tests1"
},
{
  "number":"PRBTEST002",
  "short_description":"tests2"
}
```

Multiple elements instead of an array

- Path for each row: `/problems/problem`
- Result: 3 records

**Important:** This format is not recommended. JSON files should follow RFC-4627, which states that names within an object should be unique. Use JSON arrays instead.

```
{
  "problems":{
    "title":"2 problems",
    "problem":{
      "number":"PRBTEST001",
      "short_description":"tests1"
    },
    "problem":{
      "number":"PRBTEST002",
      "short_description":"tests2"
    }
  },
  "problems":{
    "title":"1 problem",
    "problem":{
      "number":"PRBTEST005",
      "short_description":"tests5"
    }
  }
}
```

FTP data source extended properties

Certain properties are available for customizing your FTP data source.

To enter these properties, you must configure the Data Source form and add the **Properties** field. When specifying more than one property, use a comma to separate each property.
**Available FTP Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>connection.timeout</td>
<td>Defines the number of milliseconds to wait before timing out the FTP connection attempt.</td>
</tr>
<tr>
<td></td>
<td>• Default value: 10000</td>
</tr>
<tr>
<td></td>
<td>• Example custom value: connection.timeout=12000</td>
</tr>
<tr>
<td></td>
<td>• Data source: FTP, FTPS</td>
</tr>
<tr>
<td>remove_file</td>
<td>Determines if the remote file is deleted after the import.</td>
</tr>
<tr>
<td></td>
<td>• Default value: true</td>
</tr>
<tr>
<td></td>
<td>• Example custom value: remove_file=false</td>
</tr>
<tr>
<td></td>
<td>• Data source: FTP, FTPS, SFTP</td>
</tr>
<tr>
<td>rename_file</td>
<td>Determines if the remote file is renamed after the import.</td>
</tr>
<tr>
<td></td>
<td>• Default value: false</td>
</tr>
<tr>
<td></td>
<td>• Example custom value: rename_file=true</td>
</tr>
<tr>
<td></td>
<td>• Data source: FTP, FTPS, SFTP</td>
</tr>
</tbody>
</table>

**JDBC type data source**

A JDBC data source retrieves its data via a JDBC driver, usually type 4 network.

The JDBC connection is available either directly from the ServiceNow instance (a VPN setup required), or via a dedicated MID Server installed inside your firewall that can access the database port.

**Note:** JDBC calls from the MID Server are never encrypted. Limit the rights available to the MID Server user whenever making JDBC calls from a MID server.

**JDBC data source supported database formats**

JDBC data sources support several database formats and ports.

**Supported database formats**

<table>
<thead>
<tr>
<th>SQL Server Type</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>MySQL</td>
<td>3306</td>
</tr>
<tr>
<td>Microsoft SQL Server</td>
<td>1433</td>
</tr>
<tr>
<td>Oracle</td>
<td>1521</td>
</tr>
</tbody>
</table>

**Note:** Oracle DATE fields are loaded as ServiceNow Date/Time fields.
### JDBC data source SQL statement requirements

JDBC queries that run SQL statements must specify a column name.

For example, this query specifies the column name `ServerID`.

```sql
SELECT DISTINCT 'server_name:' + CONVERT ( VARCHAR , lg .ResourceID ) AS 'ServerID'
  ,LastHWScan
  ,Account0
  ,Category0
FROM v_GS_WORKSTATION_STATUS sInner 
  JOIN v_GS_LocalGroupMembers0lg
  ON s .ResourceID  = lg .ResourceID
WHERE Type0  = 'Local' AND Category0  = 'SystemAccount'
```

### SQL server integrated authentication for Windows

A JDBC data source can use the ID of for the Windows MID Server service user to authenticate with SQL Server.

The **Use integrated authentication** check box on the Data Source form determines if the JDBC data source uses the MID Server service user credentials. For this field to appear on the Data Source form, the integration must meet these criteria:

- The MID Server must be running on a Windows computer with SQL Server.
- The MID Server service must use the same credentials that SQL Server requires.
- The data source **Type** is JDBC.
- The data source **Use MID Server** check box is selected.
- The data source **Format** is SQLServer.

**Important:** If integrated authentication is chosen, and you are integrating with Microsoft System Center Configuration Manager, the account running the MID Server service must have read rights on the SCCM database.
Data Source form

**Note:** The Last run database field on the JDBC data source is case-sensitive for the SQL server.
Adding JDBC drivers for unsupported database formats

Use the following procedure to extend the data source to use a driver for a database that is not provided in the base system. JDBC connections are supported for the following default databases:

Add a new JDBC format choice

Extend the available JDBC driver options by creating a new choice list entry to specify the JDBC driver Java package name.

Role required: import_admin

Add a new choice list entry for the new database to the Format field in the sys_data_source table.

1. Navigate to System Import Sets > Administration > Data Sources.
2. Click New.
3. In the Data Sources form, right-click the Format field label, and select Show Choice List from the pop-up menu.

![Image of Data Source form with Format field expanded]
4. Click **New** in the list of choices.

5. Provide the following values to create the new database choice. Look at the existing drivers for examples.

   - **Table**: `sys_data_source`
   - **Label**: Database name that appears as an option in the **Format** choice list, for example: **Teradata**.
   - **Value**: Package name and class of the driver. For example, the value for TeraData is `com.ncr.teradata.TeraDriver`.

   **Note**: The driver package and class must be provided by the driver vendor. This information is often available in the vendor’s documentation, such as for MariaDB or Teradata.

   - **Dependent value**: JDBC

6. Click **Submit**.

The new data source now appears in the list of available JDBC formats.

**Add Sybase or DB2 JDBC format choices**

Extend the available JDBC driver options by activating the Sybase or DB2 choices.

Roles required: admin

**Important**: To use Sybase or DB2 JDBC drivers, you must manually install the driver JAR file on a MID server. Refer to KB0551236 for more information.

Activate the Sybase or DB2 JDBC drivers to connect with those database formats through a MID server. This procedure assumes you are using the following Sybase or DB2 drivers:

**Drivers**

<table>
<thead>
<tr>
<th>Format</th>
<th>Driver</th>
<th>Driver class</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sybase</td>
<td>jconnect-jdbc</td>
<td>com.sybase.jdbc3.jdbc.SybDriver</td>
</tr>
<tr>
<td>DB2</td>
<td>db2jcc</td>
<td>com.ibm.db2.jcc.DB2Driver</td>
</tr>
</tbody>
</table>
If you are using a different implementation of the Sybase or DB2 driver, you must modify the choice Value to use the driver class from your driver implementation.

1. Navigate to System Import Sets > Administration > Data Sources.
2. Click New.
3. In the Type field, select JDBC.
4. Right-click the Format field label, and select Configure Choices from the pop-up menu.
5. Move the Sybase or DB2 Universal choices from the Available column to the Selected column.
6. Click Save.

The new data source now appears in the list of available JDBC formats.

Install a driver on a MID Server
You can install a new JDBC driver JAR file to a MID server to access database formats that are not supported by default.

Role required: agent_admin

1. Navigate to MID Server > JAR Files.
2. Click New.
3. Complete the following fields:
   • Name: A unique and descriptive name for identifying the file in the instance.
   • Version: A version number for the file, if one is available.
   • Source: Location of the JAR file for reference purposes. Source information is not used by the system.
   • Description: Short description of the JAR file and its purpose in the instance.
4. Click the paper clip icon in the banner and attach the JAR file to the record.
5. Click Submit.
6. Restart the MID Server service.

The platform makes the JAR file available to any MID Server configured to communicate with the instance.

Create a new JDBC data source for an unsupported database format
Add a new JDBC data source by defining a data source record.

Role required: import_admin

1. Navigate to System Import Sets > Administration > Data Sources and click New.
2. In the Data Source form, select JDBC from the list in the Type field.
3. Select the new data source from the choice list in the **Format** field.

4. Configure the form and add the **Connection URL** field.
5. Provide the connection URL to the JDBC data source, and then click **Submit**.

No other connection information is required.
LDAP type data source

An LDAP data source is automatically created when you configure your instance to integrate with LDAP.

Processing a large LDAP request without paging

When an LDAP server does not support paging, a large request is automatically broken into multiple smaller requests. This process is known as "nibbling" the LDAP request. The large request is broken into multiple smaller requests based on the value of the Query field in the LDAP OU definition. This field should specify a unique value such as email address or user ID.

For example, the following LDAP query might return more than 1000 records.

```
(&(objectclass=user)(sn=*))
```

In this example, the LDAP server Query field is preferredIdentity. The instance then splits the large request into multiple smaller requests, grouping records based on the preferredIdentity value.

```
(&((&((preferredIdentity>=0)(preferredIdentity<=1))))(&(objectclass=user)(sn=*)))
(&((&((preferredIdentity>=1)(preferredIdentity<=2))))(&(objectclass=user)(sn=*)))
(&((&((preferredIdentity>=2)(preferredIdentity<=3))))(&(objectclass=user)(sn=*)))

...
(&((&((preferredIdentity>=9)(preferredIdentity<=a))))(&(objectclass=user)(sn=*)))
(&((&((preferredIdentity>=a)(preferredIdentity<=b))))(&(objectclass=user)(sn=*)))
(&((&((preferredIdentity>=b)(preferredIdentity<=c))))(&(objectclass=user)(sn=*)))
```

Data Stream (IntegrationHub) data source

Enable platform Data Sources to load data from IntegrationHub Data Stream actions.

A Data Stream is a stream of response data larger than 10 MB or data that returns paginated results. Successful execution of the Data Stream action returns a complex data output stream that the Data Source consumes. For more information, see Data Stream actions and pagination.
Complex data allows you to encode and store structured data in a machine-readable format. Based on Data Source configuration, complex objects can be either flattened into an import table or serialized completely as JSON data into a single column.

Complex data includes parent and child objects and nested objects, as shown in the following example:

For more information, see Complex data.

**Custom (Load by Script) type data source**

Write a custom script to store any type of incoming data in the import set table.

When you select a Type of **Custom (Load by Script)**, a Javascript field called **Data Loader** appears. You can use the data loader script to fetch data and insert it into the import set table using the **import_set_table** input parameter. Data may be obtained, for example, from a REST API or a file attachment.
The data loader script has one input parameter, `import_set_table`, and the following methods:

- **addColumn**: Adds a string type column to the import set table.
- **addJSONColumn**: Adds a JSON type column to the import set table.
- **addXMLColumn**: Adds an XML type column to the import set table.
- **insert**: Inserts a map (key = column name, value = column value) in the import set table.
- **getMaximumRows()**: Returns 20 when the user clicks **Test load 20 records**. In every other case, returns -1.

As you type the script, script auto-complete presents the choices available to you, as shown in this example:

---

**Create a data source**

Create a data source record to define what data an import set should import.

Depending on the type of data source you want to create, see the following topics for procedures.

*Create a File type data source*

Create a **File** type data source record to define what data an import set should import.

Role required: import_admin

For additional information, see [File type data sources](#).

1. Navigate to **System Import Sets > Administration > Data Sources**.
2. Click **New**.
3. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name for this data source.</td>
</tr>
<tr>
<td>Import set table label</td>
<td>A label for the import set staging table to use.</td>
</tr>
<tr>
<td>Import set table name</td>
<td>The label you entered to construct a unique table name. This prevents namespace collision with an already existing table.</td>
</tr>
<tr>
<td>Type</td>
<td><strong>File.</strong></td>
</tr>
<tr>
<td>Format</td>
<td>Only the default XML-based file format (.xlsx) is supported, unless saved as &quot;Strict Open XML Document.&quot;</td>
</tr>
<tr>
<td>Zipped</td>
<td>Selected if the import file is compressed.</td>
</tr>
<tr>
<td>Use Batch Import</td>
<td>If selected, specifies that loading data should be batched when you click <strong>Load data</strong> or <strong>Test load 20 records</strong>.</td>
</tr>
<tr>
<td>Batch Size</td>
<td>Specifies how big the batches should be. Appears only when the <strong>Use Batch Import</strong> field is selected.</td>
</tr>
<tr>
<td></td>
<td>The <strong>glide.import_set_load_usebatch</strong> and <strong>glide.import_set_load_batch_size</strong> properties affect these fields. The priority order for the properties and fields are as follows: If the property is set, use the property value. If not, use the field value. If neither property is set, use the default batch size of 1000.</td>
</tr>
<tr>
<td></td>
<td>• For example, if <strong>glide.import_set_load_usebatch</strong> = <strong>true</strong> and <strong>glide.import_set_load_batch_size</strong> = <strong>200</strong>, use 200 as the batch size, regardless of the field values.</td>
</tr>
<tr>
<td></td>
<td>• For example, if <strong>glide.import_set_load_usebatch</strong> = <strong>true</strong> and the <strong>glide.import_set_load_batch_size</strong> property is not set, use the default batch size of 1000.</td>
</tr>
<tr>
<td></td>
<td>• For example, if the <strong>glide.import_set_load_usebatch</strong> property is not set and the <strong>Use Batch Import</strong> field = <strong>true</strong>, use the <strong>Batch Size</strong> field value (or the default of 1000 if the <strong>Batch Size</strong> field value is not set)</td>
</tr>
<tr>
<td></td>
<td>• For example, if the <strong>glide.import_set_load_usebatch</strong> property = <strong>false</strong> and the <strong>Use Batch Import</strong> field = <strong>true</strong>, do not use batch import, since the property is set to false.</td>
</tr>
<tr>
<td>File retrieval method</td>
<td>The retrieval method for this file.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>File path</td>
<td>The path to the file to import. You can include a system property value in this field using the format <code>${system.property.name}</code>. When the connection is made, the variable is replaced with the value of the specified property.</td>
</tr>
<tr>
<td>Note: For files retrieved using HTTP or HTTPS, the <code>glide.ds.file.http.variable_replacement</code> property must be true to use system property expansion.</td>
<td></td>
</tr>
<tr>
<td>For example, you can specify the file path value <code>/countries.csv?key=${datasource.apikey}</code>. When the connection is made, the value of the <code>datasource.apikey</code> system property is passed as the value for the key parameter.</td>
<td></td>
</tr>
<tr>
<td>Note: For HTTP and HTTPS protocols, the file path is automatically URL encoded. Do not specify a URL-encoded file path when using either of these protocols.</td>
<td></td>
</tr>
<tr>
<td>CSV delimiter</td>
<td>The delimiter character for the CSV file.</td>
</tr>
<tr>
<td>Parsing script</td>
<td>The script used to parse a single line of input. As you type the script, script auto-complete presents the choices available to you. For more information, see File type data sources.</td>
</tr>
<tr>
<td>Sheet number</td>
<td>The Excel sheet number to load data.</td>
</tr>
<tr>
<td>Header row</td>
<td>The Excel sheet number to load the column labels.</td>
</tr>
<tr>
<td>Path for each row</td>
<td>The path expression used to select JSON objects, which will become rows in the import set table. The path should be <code>//</code> for JSON objects.</td>
</tr>
<tr>
<td>Discard Arrays</td>
<td>Selected to discard JSON arrays as a value. Unselected to serialize JSON arrays as a value.</td>
</tr>
<tr>
<td>Expand node children</td>
<td>Selected if child elements of the XML node or JSON object should be converted into additional columns. Unselected if the parent column value should be an XML or JSON fragment. For JSON, note that selecting this option expands objects only, not arrays. For nested array support, see Importing JSON files.</td>
</tr>
<tr>
<td>Data in single column</td>
<td>Selected to store data in a single column.</td>
</tr>
<tr>
<td>Xpath for each row</td>
<td>XPath expression that selects the nodes which become rows in the import table. The children of the selected nodes will become the columns in the rows.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
SCP authentication method | Choice to authenticate with a username and password or with a public key.

**Note:** You cannot authenticate to data sources with a public-private key pair. Use a username and password authentication instead.

Server | Name of the server from which the tables will be imported.
Port | Port to use to connect to the specified server. This field appears if you select HTTP or HTTPS as the file retrieval method.
Username | User name for authentication on the JDBC server.
Password | Password for authentication on the JDBC server.
Private keyfile | Keyfile when using legacy SCP public-private keyfiles.

**Note:**
- You cannot authenticate to data sources with a public-private key pair. Use username and password authentication instead.
- Do not use this legacy option. Although it is available for use, it is not supported.

System keystore | Selected to validate the certificate from the FTPS server against all saved certificates. This certificate may be any type supported by the instance. If not selected, the instance uses the Java default certificate to validate the FTPS server. This field is available only for data sources with a **File retrieval method** value of **FTPS**. All FTPS file retrieval methods are supported, including Auth TLS, Auth SSL, Implicit SSL, and Implicit TLS.

4. Click **Submit**.

Define a transform map for the new data source and run an import.

*Create a JDBC type data source*

Create a **JDBC** type data source record to define what data an import set should import.

Role required: import_admin

For additional information, see **JDBC type data source**.

1. Navigate to **System Import Sets > Administration > Data Sources**.
2. Click **New**.
3. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name for this data source.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Import set table label</td>
<td>A label for the import set staging table to use.</td>
</tr>
<tr>
<td>Import set table name</td>
<td>The label you entered to construct a unique table name. This prevents namespace collision with an already existing table.</td>
</tr>
<tr>
<td>Type</td>
<td><strong>JDBC</strong>.</td>
</tr>
<tr>
<td>Use MID Server</td>
<td>MID Server to use to connect to this data source.</td>
</tr>
<tr>
<td>Format</td>
<td>Select one of the following formats: MySQL, Oracle, or SQLServer.</td>
</tr>
<tr>
<td>Instance name</td>
<td>Used to support dynamic port connectivity with SQL Server. To ensure connectivity, provide the instance name for a SQL Server that receives a new port number dynamically after each reboot. This field only appears when <strong>SQLServer</strong> is selected as a data source format.</td>
</tr>
<tr>
<td>Database name</td>
<td>Name of the database instance.</td>
</tr>
<tr>
<td>Database port</td>
<td>Port number for the database. Leave this field empty when using dynamic port connectivity with SQL Server.</td>
</tr>
<tr>
<td>Use Batch Import</td>
<td>If selected, specifies that loading data should be batched when you click <strong>Load data</strong> or <strong>Test load 20 records</strong>.</td>
</tr>
<tr>
<td>Batch Size</td>
<td>Specifies how big the batches should be. Appears only when the <strong>Use Batch Import</strong> field is selected.</td>
</tr>
</tbody>
</table>

The **glide.import_set_load_usebatch** and **glide.import_set_load_batch_size** properties affects these fields. The priority order for the properties and fields are as follows: If the property is set, use the property value. If not, use the field value. If neither property is set, use the default batch size of 1000.

- For example, if 
  
  glide.import_set_load_usebatch = true and 
  glide.import_set_load_batch_size = 200,
  
  use 200 as the batch size, regardless of the field values.

- For example, if 
  
  glide.import_set_load_usebatch = true and the glide.import_set_load_batch_size property is not set, use the default batch size of 1000.

- For example, if the 
  
  glide.import_set_load_usebatch property is not set and the **Use Batch Import** field = true,
  
  use the **Batch Size** field value (or the default of 1000 if the **Batch Size** field value is not set)

- For example, if the 
  
  glide.import_set_load_usebatch property = false and the **Use Batch Import** field = true, do not use batch import, since the property is set to false.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use integrated authentication</td>
<td>Selected to allow the JDBC connection to use the ID of the user configured for the Windows MID Server service for SQL Server authentication. For additional details, see <a href="#">JDBC type data source</a>.</td>
</tr>
<tr>
<td>Username</td>
<td>User name for authentication on the JDBC server.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for authentication on the JDBC server.</td>
</tr>
<tr>
<td>Server</td>
<td>Name of the server from which the tables will be imported.</td>
</tr>
<tr>
<td>Query</td>
<td>Type of query to run: <strong>All rows from Table</strong> or <strong>Specific SQL</strong>. If you select to run a SQL statement, the SQL statement field appears.</td>
</tr>
<tr>
<td>Query timeout</td>
<td>Number of seconds the JDBC driver will wait for a query (SELECT) to complete. Zero (0) means no timeout. If timeout is exceeded, the integration considers the JDBC result inaccessible and places it in an error state.</td>
</tr>
<tr>
<td>Connection timeout</td>
<td>Number of seconds before MID Server connection cache pool closes and removes it from the pool. Zero (0) means no timeout.</td>
</tr>
<tr>
<td>Table name</td>
<td>Name of the table from which the data is being exported.</td>
</tr>
<tr>
<td>SQL statement</td>
<td>SQL statement to extract the desired data from the database.</td>
</tr>
<tr>
<td>Use last run datetime</td>
<td>Controls the amount of data that is retrieved from a database during an import run. If unselected, then all rows in the table specified are imported, every time. You might want to use this setting if this is a one-time import, or if all the data in the target table is new. If selected, two additional fields appear, enabling you to select a datetime value to limit imported data to delta values only.</td>
</tr>
<tr>
<td>Last run datetime</td>
<td>The datetime value in this field is automatically populated from the database field you select below and represents the latest value from the previous run. This value acts as a dynamic filter to restrict the number of records retrieved to those records that have changed since the data source’s last runtime.</td>
</tr>
<tr>
<td>Last run database field</td>
<td>Field name from the source table that will be used as the filter in the next run. This value may need to be case sensitive, depending on the target database type.</td>
</tr>
<tr>
<td>Additional Database Parameters</td>
<td>Optional parameters to add to the end of the URL generated for this data source. Semicolon-separated list of parameters. You may need to configure the form to view this field.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

Define a transform map for the new data source and run an import.

*Create an LDAP type data source*

Create an **LDAP** type data source record to define what data an import set should import.

Role required: import_admin
For additional information, see LDAP type data source.

1. Navigate to **System Import Sets > Administration > Data Sources**.
2. Click **New**.
3. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name for this data source.</td>
</tr>
<tr>
<td>Import set table label</td>
<td>A label for the import set staging table to use.</td>
</tr>
<tr>
<td>Import set table name</td>
<td>The uses the label you entered to construct a unique table name. This prevents namespace collision with an already existing table.</td>
</tr>
<tr>
<td>Type</td>
<td>LDAP.</td>
</tr>
<tr>
<td>LDAP target</td>
<td>Target selected from the list of your LDAP OU definitions.</td>
</tr>
<tr>
<td>Use Batch Import</td>
<td>If selected, specifies that loading data should be batched when you click Load data or Test load 20 records.</td>
</tr>
<tr>
<td>Batch Size</td>
<td>Specifies how big the batches should be. Appears only when the Use Batch Import field is selected.</td>
</tr>
</tbody>
</table>

The glide.import_set_load_usebatch and glide.import_set_load_batch_size properties affects these fields. The priority order for the properties and fields are as follows: If the property is set, use the property value. If not, use the field value. If neither property is set, use the default batch size of 1000.

- For example, if glide.import_set_load_usebatch = true and glide.import_set_load_batch_size = 200, use 200 as the batch size, regardless of the field values.
- For example, if glide.import_set_load_usebatch = true and the glide.import_set_load_batch_size property is not set, use the default batch size of 1000.
- For example, if the glide.import_set_load_usebatch property is not set and the Use Batch Import field = true, use the Batch Size field value (or the default of 1000 if the Batch Size field value is not set)
- For example, if the glide.import_set_load_usebatch property = false and the Use Batch Import field = true, do not use batch import, since the property is set to false.

4. Click **Submit**.

Define a transform map for the new data source and run an import.
Create an OIDC type data source
Create an **OIDC** type data source record to define what data an import set should import.

Role required: import_admin

1. Navigate to **System Import Sets > Administration > Data Sources**.
2. Click **New**.
3. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name for this data source.</td>
</tr>
<tr>
<td>Import set table label</td>
<td>A label for the import set staging table to use.</td>
</tr>
<tr>
<td>Import set table name</td>
<td>The uses the label you entered to construct a unique table name. This prevents namespace collision with an already existing table.</td>
</tr>
<tr>
<td>Type</td>
<td>OIDC.</td>
</tr>
<tr>
<td>Use Batch Import</td>
<td>If selected, specifies that loading data should be batched when you click Load data or Test load 20 records.</td>
</tr>
</tbody>
</table>
| Batch Size          | Specifies how big the batches should be. Appears only when the Use Batch Import field is selected. The **glide.import_set_load_usebatch** and **glide.import_set_load_batch_size** properties affects these fields. The priority order for the properties and fields are as follows: If the property is set, use the property value. If not, use the field value. If neither property is set, use the default batch size of 1000.

- For example, if **glide.import_set_load_usebatch** = true and **glide.import_set_load_batch_size** = 200, use 200 as the batch size, regardless of the field values.
- For example, if **glide.import_set_load_usebatch** = true and the **glide.import_set_load_batch_size** property is not set, use the default batch size of 1000.
- For example, if the **glide.import_set_load_usebatch** property is not set and the **Use Batch Import** field = true, use the **Batch Size** field value (or the default of 1000 if the **Batch Size** field value is not set)
- For example, if the **glide.import_set_load_usebatch** property = false and the **Use Batch Import** field = true, do not use batch import, since the property is set to false.

| Format                          | Defaults to **-- None --** and can't be changed.                            |

4. Click **Submit**.

Define a transform map for the new data source and run an import.
Create a REST (IntegrationHub) type data source

Create a **REST (IntegrationHub)** type data source record to define what data an import set should import from a REST API.

Roles required: import_admin and action_designer

1. Navigate to **System Import Sets > Administration > Data Sources**.
2. Click **New**.
3. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name for this data source.</td>
</tr>
<tr>
<td>Import set table label</td>
<td>A label for the import set staging table to use.</td>
</tr>
<tr>
<td>Import set table name</td>
<td>The uses the label you entered to construct a unique table name. This prevents namespace collision with an already existing table.</td>
</tr>
<tr>
<td>Type</td>
<td>REST (IntegrationHub)</td>
</tr>
<tr>
<td>Format</td>
<td>One of the following formats: Custom (Parse by Script), JSON, or XML.</td>
</tr>
<tr>
<td>Use Batch Import</td>
<td>If selected, specifies that loading data should be batched when you click <strong>Load data</strong> or <strong>Test load 20 records</strong>.</td>
</tr>
<tr>
<td>Batch Size</td>
<td>Specifies how big the batches should be. Appears only when the <strong>Use Batch Import</strong> field is selected.</td>
</tr>
</tbody>
</table>

The **glide.import_set_load_usebatch** and **glide.import_set_load_batch_size** properties affect these fields. The priority order for the properties and fields are as follows: If the property is set, use the property value. If not, use the field value. If neither property is set, use the default batch size of 1000.

- For example, if **glide.import_set_load_usebatch = true** and **glide.import_set_load_batch_size = 200**, use 200 as the batch size, regardless of the field values.
- For example, if **glide.import_set_load_usebatch = true** and the **glide.import_set_load_batch_size** property is not set, use the default batch size of 1000.
- For example, if the **glide.import_set_load_usebatch** property is not set and the **Use Batch Import** field = **true**, use the **Batch Size** field value (or the default of 1000 if the **Batch Size** field value is not set).
- For example, if the **glide.import_set_load_usebatch** property = **false** and the **Use Batch Import** field = **true**, do not use batch import, since the property is set to false.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request action</td>
<td>Data source request action that will be invoked to get data. You can choose only published request actions. Click the link in the dialog box below to create/configure a new Data Source request action in . After the request action is published in , you can choose it as a Request action in the Data Source record. For more information, see Define action properties.</td>
</tr>
<tr>
<td>Support pagination</td>
<td>Selected to enable pagination for the request action. Pagination helps you reduce processing overhead by processing a specified number of records at a time, instead of processing all records at once.</td>
</tr>
<tr>
<td>Limit</td>
<td>Maximum number of records per page. For example, to process 50 records at a time, enter a Limit of 50.</td>
</tr>
<tr>
<td>Offset</td>
<td>The initial offset used for pagination. The offset is the starting record number. For example, to process 50 records at a time, starting with the first record, enter a Limit of 50 and an Offset of 0.</td>
</tr>
<tr>
<td>Parsing script</td>
<td>Type the script used to parse a single line of input. Three parameters are available in this function: • line: the current line to be parsed by the script • lineNumber: the line number of the current line in the entire response payload • result: output result</td>
</tr>
<tr>
<td>Path for each row</td>
<td>The path expression used to select JSON objects, which will become rows in the import set table. The path should be // for JSON objects.</td>
</tr>
<tr>
<td>Discard Arrays</td>
<td>Selected to discard JSON arrays as a value. Unselected to serialize JSON arrays as a value.</td>
</tr>
<tr>
<td>Expand node children</td>
<td>Selected if child elements of the XML node or JSON object should be converted into additional columns. Unselected if the parent column value should be an XML or JSON fragment. For JSON, note that selecting this option expands objects only, not arrays. For nested array support, see Importing JSON files.</td>
</tr>
<tr>
<td>Data in single column</td>
<td>Selected to store data in a single column.</td>
</tr>
<tr>
<td>Xpath for each row</td>
<td>XPath expression that selects the nodes which become rows in the import table. The children of the selected nodes will become the columns in the rows.</td>
</tr>
</tbody>
</table>

4. Click Submit.

Define a transform map for the new data source and run an import.

Define action properties
Create and configure a Data Source request action in IntegrationHub. After the request action is published in IntegrationHub, you can choose it as a Request action in the Data Source record.

Role required: import_admin

1. Navigate to System Import Sets > Administration > Data Sources.
2. Select New.
3. Select a **Type** of **REST** *(IntegrationHub)*.
4. Click the link under **Request action**.
5. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the request action.</td>
</tr>
<tr>
<td>Accessible From</td>
<td>Scope from which the request action is accessible.</td>
</tr>
<tr>
<td>Category</td>
<td>Category of the request action.</td>
</tr>
<tr>
<td>Protection</td>
<td>Specifies whether the request action is read-only.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the request action.</td>
</tr>
<tr>
<td>Application</td>
<td>Scope of the application.</td>
</tr>
<tr>
<td>In-Flow Annotation</td>
<td>Text you want to appear under the <strong>Action</strong> title on the Data Source Request Action page.</td>
</tr>
</tbody>
</table>

6. Click **Submit**.
7. The Data Source Request Action page appears with the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limit</td>
<td>Limit set by the user in the REST <em>(IntegrationHub)</em> data source record. If the REST API supports pagination and <strong>Support pagination</strong> is selected in the Data Source record, you must supply this input to your REST step.</td>
</tr>
<tr>
<td>Offset</td>
<td>Offset set by user in the REST <em>(IntegrationHub)</em> data source record. If the REST API supports pagination and <strong>Support pagination</strong> is selected in the Data Source record, you must supply this input to your REST step.</td>
</tr>
<tr>
<td>Last Success Import Time</td>
<td>Last time data was successfully imported. A numeric value representing the number of milliseconds since January 1, 1970, 00:00:00 GMT. The data source populates this value. If the REST API supports queries based on time, you must supply this input to your REST step.</td>
</tr>
<tr>
<td>Import Start Time</td>
<td>Time the import is actually started. A numeric value representing the number of milliseconds since January 1, 1970, 00:00:00 GMT. The data source populates this value. If the REST API supports queries based on time, you must supply this input to your REST step.</td>
</tr>
</tbody>
</table>

8. If desired, you can add a Script step to validate or modify action inputs, set default values, or build request payloads before executing the REST step.
   a) Select **Data Source Request** from the Action Outline.
   b) Select **Enable Processing Script**.
   c) Select **Script step** from the Action Outline.
   d) Configure the Script step as described in **Script step**.

9. Select **REST step** from the Action Outline.
10. Configure the REST step as described in **REST step**.
11. Choose from the following:
   • Click **Properties** to return to the Action Properties window.
   • Click **Test** to test the request action before publishing it.
   • Click **Executions** to view the history of executions of the request action.
   • Click **Save** to save the request action.
   • Click **Publish** to publish the request action and make it available for use.

Create a Data Stream (IntegrationHub) type data source

Create a **Data Stream (IntegrationHub)** type data source record to define what complex data an import set should import from a Data Stream action.

Role required: import_admin and action_designer

1. Navigate to **System Import Sets > Administration > Data Sources**.
2. Click **New**.
3. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name for this data source.</td>
</tr>
<tr>
<td>Import set table label</td>
<td>A label for the import set staging table to use.</td>
</tr>
<tr>
<td>Import set table name</td>
<td>The uses the label you entered to construct a unique table name. This prevents namespace collision with an already existing table.</td>
</tr>
<tr>
<td>Type</td>
<td>Data Stream () type data source.</td>
</tr>
<tr>
<td>Data Stream action</td>
<td>• Selected to use an existing published Data Stream action from .</td>
</tr>
<tr>
<td></td>
<td>• Selected for one of the following reasons:</td>
</tr>
<tr>
<td>Data in single column</td>
<td>Selected to store data in a single column.</td>
</tr>
<tr>
<td>Use Batch Import</td>
<td>If selected, specifies that loading data should be batched when you click <strong>Load data</strong> or <strong>Test load 20 records</strong>.</td>
</tr>
</tbody>
</table>
### Field Description

**Batch Size**
- Specifies how big the batches should be. Appears only when the **Use Batch Import** field is selected.

The `glide.import_set.load.usebatch` and `glide.import_set.load.batch_size` properties affect these fields. The priority order for the properties and fields are as follows: If the property is set, use the property value. If not, use the field value. If neither property is set, use the default batch size of 1000.

- For example, if `glide.import_set.load.usebatch = true` and `glide.import_set.load.batch_size = 200`, use 200 as the batch size, regardless of the field values.
- For example, if `glide.import_set.load.usebatch = true` and the `glide.import_set.load.batch_size` property is not set, use the default batch size of 1000.
- For example, if the `glide.import_set.load.usebatch` property is not set and the **Use Batch Import** field = true, use the **Batch Size** field value (or the default of 1000 if the **Batch Size** field value is not set).
- For example, if the `glide.import_set.load.usebatch` property = false and the **Use Batch Import** field = true, do not use batch import, since the property is set to false.

---

**Data Stream action inputs**
- Additional fields may appear, based on the inputs defined in the **Data Stream action**.

### 4. Click **Submit**.

Define a transform map for the new data source and run an import.

*Create a Custom (Load by Script) type data source*

Create a **Custom (Load by Script)** type data source record to define what data an import set should import.

**Role required:** import_admin

For additional information, see **Custom (Load by Script) type data source**.

1. Navigate to **System Import Sets > Administration > Data Sources**.
2. Click **New**.
3. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name for this data source.</td>
</tr>
<tr>
<td>Import set table label</td>
<td>A label for the import set staging table to use.</td>
</tr>
<tr>
<td>Import set table name</td>
<td>The uses the label you entered to construct a unique table name. This prevents namespace collision with an already existing table.</td>
</tr>
<tr>
<td>Type</td>
<td><strong>Custom (Load by Script)</strong>.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Use Batch Import | If selected, specifies that loading data should be batched when you click **Load data** or **Test load 20 records**.
Batch Size | Specifies how big the batches should be. Appears only when the **Use Batch Import** field is selected.

The `glide.import_set_load_usebatch` and `glide.import_set_load_batch_size` properties affect these fields. The priority order for the properties and fields are as follows: If the property is set, use the property value. If not, use the field value. If neither property is set, use the default batch size of 1000.

- For example, if `glide.import_set_load_usebatch = true` and `glide.import_set_load_batch_size = 200`, use 200 as the batch size, regardless of the field values.
- For example, if `glide.import_set_load_usebatch = true` and the `glide.import_set_load_batch_size` property is not set, use the default batch size of 1000.
- For example, if the `glide.import_set_load_usebatch` property is not set and the **Use Batch Import** field = true, use the **Batch Size** field value (or the default of 1000 if the **Batch Size** field value is not set)
- For example, if the `glide.import_set_load_usebatch` property = false and the **Use Batch Import** field = true, do not use batch import, since the property is set to false.

### Data Loader
Script used to load data. For more information, see [Custom (Load by Script) type data source](https:// servicenow.com).

4. Click **Submit**.

Define a transform map for the new data source and run an import.

### Data source fields
In addition to common fields, other fields appear on the data source form, depending on the value of the **Type** field.

### Common data source fields
These fields are common to all data sources.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name for this data source.</td>
</tr>
<tr>
<td>Import set table label</td>
<td>A label for the import set staging table to use.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Import set table name</td>
<td>The uses the label you entered to construct a unique table name. This prevents namespace collision with an already existing table.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of data you are importing:</td>
</tr>
<tr>
<td></td>
<td>• From a remote File</td>
</tr>
<tr>
<td></td>
<td>• From a JDBC database</td>
</tr>
<tr>
<td></td>
<td>• Using LDAP</td>
</tr>
<tr>
<td></td>
<td>• Using OIDC</td>
</tr>
<tr>
<td></td>
<td>• Using REST to import data through the IntegrationHub</td>
</tr>
<tr>
<td></td>
<td>• From a Data Stream action through the</td>
</tr>
<tr>
<td></td>
<td>• Using a Custom script</td>
</tr>
<tr>
<td>Use Batch Import</td>
<td>If selected, specifies that loading data should be batched when you click Load data or Test load 20 records.</td>
</tr>
<tr>
<td>Batch Size</td>
<td>Specifies how big the batches should be. Appears only when the Use Batch Import field is selected.</td>
</tr>
<tr>
<td></td>
<td>The glide.import_set_load_usebatch and glide.import_set_load_batch_size properties affects these fields. The priority order for the properties and fields are as follows: If the property is set, use the property value. If not, use the field value. If neither property is set, use the default batch size of 1000.</td>
</tr>
<tr>
<td></td>
<td>• For example, if glide.import_set_load_usebatch = true and glide.import_set_load_batch_size = 200, use 200 as the batch size, regardless of the field values.</td>
</tr>
<tr>
<td></td>
<td>• For example, if glide.import_set_load_usebatch = true and the glide.import_set_load_batch_size property is not set, use the default batch size of 1000.</td>
</tr>
<tr>
<td></td>
<td>• For example, if the glide.import_set_load_usebatch property is not set and the Use Batch Import field = true, use the Batch Size field value (or the default of 1000 if the Batch Size field value is not set)</td>
</tr>
<tr>
<td></td>
<td>• For example, if the glide.import_set_load_usebatch property = false and the Use Batch Import field = true, do not use batch import, since the property is set to false.</td>
</tr>
<tr>
<td>Application</td>
<td>Application scope for this record.</td>
</tr>
</tbody>
</table>

**File type data source fields**

These additional fields appear on the data source form when the **Type** field value is **File**.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>Only the default XML-based file format (.xlsx) is supported, unless saved as “Strict Open XML Document.”</td>
</tr>
<tr>
<td>Zipped</td>
<td>Selected if the import file is compressed.</td>
</tr>
<tr>
<td>File retrieval method</td>
<td>The retrieval method for this file.</td>
</tr>
<tr>
<td>File path</td>
<td>The path to the file to import. You can include a system property value in this field using the format ${\text{system.property.name}}$. When the connection is made, the variable is replaced with the value of the specified property.</td>
</tr>
<tr>
<td></td>
<td>For example, you can specify the file path value <code>/countries.csv?key=${datasource.apikey}</code>. When the connection is made, the value of the <code>datasource.apikey</code> system property is passed as the value for the <code>key</code> parameter.</td>
</tr>
<tr>
<td>CSV delimiter</td>
<td>The delimiter character for the CSV file.</td>
</tr>
<tr>
<td>Parsing script</td>
<td>The script used to parse a single line of input. As you type the script, script auto-complete presents the choices available to you. For more information, see File type data sources.</td>
</tr>
<tr>
<td>Sheet number</td>
<td>The Excel sheet number to load data.</td>
</tr>
<tr>
<td>Header row</td>
<td>The Excel sheet number to load the column labels.</td>
</tr>
<tr>
<td>Path for each row</td>
<td>The path expression used to select JSON objects, which will become rows in the import set table. The path should be // for JSON objects.</td>
</tr>
<tr>
<td>Discard Arrays</td>
<td>Selected to discard JSON arrays as a value. Unselected to serialize JSON arrays as a value.</td>
</tr>
<tr>
<td>Expand node children</td>
<td>Selected if child elements of the XML node or JSON object should be converted into additional columns. Unselected if the parent column value should be an XML or JSON fragment. For JSON, note that selecting this option expands objects only, not arrays. For nested array support, see Importing JSON files.</td>
</tr>
<tr>
<td>Data in single column</td>
<td>Selected to store data in a single column.</td>
</tr>
<tr>
<td>Xpath for each row</td>
<td>XPath expression that selects the nodes which become rows in the import table. The children of the selected nodes will become the columns in the rows.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| SCP authentication method   | Choice to authenticate with a username and password or with a public key.  
|                             | **Note:** You cannot authenticate to data sources with a public-private key pair. Use a username and password authentication instead.         |
| Server                      | Name of the server from which the tables will be imported.  
| Port                        | Port to use to connect to the specified server. This field appears if you select HTTP or HTTPS as the file retrieval method.                    |
| Username                    | User name for authentication on the JDBC server.                                                                                                                                                      |
| Password                    | Password for authentication on the JDBC server.                                                                                                                                                       |
| Private keyfile             | Keyfile when using legacy SCP public-private keyfiles.  
|                             | **Note:**  
|                             | • You cannot authenticate to data sources with a public-private key pair. Use username and password authentication instead.  
| System keystore             | Selected to validate the certificate from the FTPS server against all saved certificates. This certificate may be any type supported by the instance. If not selected, the instance uses the Java default certificate to validate the FTPS server. This field is available only for data sources with a File retrieval method value of FTPS. All FTPS file retrieval methods are supported, including Auth TLS, Auth SSL, Implicit SSL, and Implicit TLS. |

### JDBC type data source fields

These additional fields appear on the data source form when the **Type** field value is **JDBC**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use MID Server</td>
<td>MID Server to use to connect to this data source.</td>
</tr>
<tr>
<td>Format</td>
<td>One of the following formats: MySQL, Oracle, or SQLServer.</td>
</tr>
<tr>
<td>Instance name</td>
<td>Used to support dynamic port connectivity with SQL Server. To ensure connectivity, provide the instance name for a SQL Server that receives a new port number dynamically after each reboot. This field only appears when SQLServer is selected as a data source format.</td>
</tr>
<tr>
<td>Database name</td>
<td>Name of the database instance.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Database port</td>
<td>Port number for the database. Leave this field empty when using dynamic port connectivity with SQL Server.</td>
</tr>
<tr>
<td>Use integrated</td>
<td>Selected to allow the JDBC connection to use the ID of the user configured for the Windows MID Server service for SQL Server authentication. For additional details, see JDBC type data source.</td>
</tr>
<tr>
<td>authentication</td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td>User name for authentication on the JDBC server.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for authentication on the JDBC server.</td>
</tr>
<tr>
<td>Server</td>
<td>Name of the server from which the tables will be imported.</td>
</tr>
<tr>
<td>Query</td>
<td>Type of query to run: <strong>All rows from Table</strong> or <strong>Specific SQL</strong>. If you select to run a SQL statement, the SQL statement field appears.</td>
</tr>
<tr>
<td>Query timeout</td>
<td>Number of seconds the JDBC driver will wait for a query (SELECT) to complete. Zero (0) means no timeout. If timeout is exceeded, the integration considers the JDBC result inaccessible and places it in an error state.</td>
</tr>
<tr>
<td>Connection timeout</td>
<td>Number of seconds before MID Server connection cache pool closes and removes it from the pool. Zero (0) means no timeout.</td>
</tr>
<tr>
<td>Table name</td>
<td>Name of the table from which the data is being exported.</td>
</tr>
<tr>
<td>SQL statement</td>
<td>SQL statement to extract the desired data from the database.</td>
</tr>
<tr>
<td>Use last run</td>
<td>Controls the amount of data that is retrieved from a database during an import run. If unselected, then all rows in the table specified are imported, every time. You might want to use this setting if this is a one-time import, or if all the data in the target table is new. If selected, two additional fields appear, enabling you to select a datetime value to limit imported data to delta values only.</td>
</tr>
<tr>
<td>datetime</td>
<td></td>
</tr>
<tr>
<td>Last run datetime</td>
<td>The datetime value in this field is automatically populated from the database field you select below and represents the latest value from the previous run. This value acts as a dynamic filter to restrict the number of records retrieved to those records that have changed since the data source's last runtime.</td>
</tr>
<tr>
<td>Last run database</td>
<td>Field name from the source table that will be used as the filter in the next run. This value may need to be case sensitive, depending on the target database type.</td>
</tr>
<tr>
<td>Additional Database</td>
<td>Optional parameters to add to the end of the URL generated for this data source. Semicolon-separated list of parameters. You may need to configure the form to view this field.</td>
</tr>
<tr>
<td>Parameters</td>
<td></td>
</tr>
</tbody>
</table>

**LDAP type data source field**

This additional field appears on the data source form when the **Type** field value is **LDAP**.
### OIDC type data source field

This additional field appears on the data source form when the Type field value is **OIDC**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>Defaults to <strong>-- None --</strong> and can’t be changed.</td>
</tr>
</tbody>
</table>

### REST (IntegrationHub) type data source fields

These additional fields appear on the data source form when the Type field value is **REST (IntegrationHub)**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>One of the following formats: Custom (Parse by Script), JSON, or XML.</td>
</tr>
<tr>
<td>Request action</td>
<td>Data source request action that will be invoked to get data. You can choose only published request actions. Click the link in the dialog box below to create/configure a new Data Source request action in . After the request action is published in , you can choose it as a Request action in the Data Source record. For more information, see Define action properties.</td>
</tr>
<tr>
<td>Support pagination</td>
<td>Selected to enable pagination for the request action. Pagination helps you reduce processing overhead by processing a specified number of records at a time, instead of processing all records at once.</td>
</tr>
<tr>
<td>Limit</td>
<td>Maximum number of records per page. For example, to process 50 records at a time, enter a Limit of 50.</td>
</tr>
<tr>
<td>Offset</td>
<td>The initial offset used for pagination. The offset is the starting record number. For example, to process 50 records at a time, starting with the first record, enter a Limit of 50 and an Offset of 0.</td>
</tr>
<tr>
<td>Parsing script</td>
<td>The script used to parse a single line of input. As you type the script, script auto-complete presents the choices available to you. For more information, see File type data sources.</td>
</tr>
<tr>
<td>Path for each row</td>
<td>The path expression used to select JSON objects, which will become rows in the import set table. The path should be / / for JSON objects.</td>
</tr>
<tr>
<td>Discard Arrays</td>
<td>Selected to discard JSON arrays as a value. Unselected to serialize JSON arrays as a value.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Expand node children</td>
<td>Selected if child elements of the XML node or JSON object should be converted into additional columns. Unselected if the parent column value should be an XML or JSON fragment. For JSON, note that selecting this option expands objects only, not arrays. For nested array support, see Importing JSON files.</td>
</tr>
<tr>
<td>Data in single column</td>
<td>Selected to store data in a single column.</td>
</tr>
<tr>
<td>Xpath for each row</td>
<td>XPath expression that selects the nodes which become rows in the import table. The children of the selected nodes will become the columns in the rows.</td>
</tr>
</tbody>
</table>

### Data Stream (IntegrationHub) type data source fields

These additional fields appear on the data source form when the **Type** field value is **Data Stream (IntegrationHub)**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Data Stream () type data source.</td>
</tr>
</tbody>
</table>
| Data Stream action  | • ![Search icon](image)  
Selected to use an existing published Data Stream action from .  
• ![Arrow icon](image)  
Selected for one of the following reasons:  
• If you select a published Data Stream action, click this button to open the Data Stream action in .  
• If you don't select a Data Stream action, click this button to create and publish a new Data Stream action in .  

**Note:** Data Stream actions require a subscription for production use.  

| Data in single column | Selected to store data in a single column.                                                                                                                                                                                                                                                                                                   |
| Data Stream action inputs | Additional fields may appear, based on the inputs defined in the Data Stream action.                                                                                                                                                                                                                                               |

### Custom (Load by Script) type data source field

This additional field appears on the data source form when the **Type** field value is **Custom (Load by Script)**.
### Transform maps

A transform map is a set of field maps that determine the relationships between fields in an import set and fields in an existing ServiceNow table, such as Incident [incident] or User [sys_user].

![Diagram of transform maps and data sources](image)

#### Import process transform

After creating a transform map, you can reuse it to map data from another import set to the same table. The Transform Maps module enables an administrator to define destinations for imported data on any tables. Transform mapping can be as simple as a drag and drop operation to specify linking between source fields on an import set table and destination fields on any table. Use transform mapping to map source and destination fields dynamically.
Transform considerations

**Auto-mapping**

Double-check that fields the system maps automatically are actually required. For example, encrypted passwords probably should not be mapped.

**Mapping reference fields**

If you are mapping reference field data and the sys_id does not exist, the sys_id could potentially appear in the target record as the DisplayValue, and this may be undesirable.

Field mapping a large number of reference fields incurs additional performance overhead because the system checks that the referenced sys_id actually exists before performing choice actions at the field level.

**Note:** You can bypass the performance overhead using transform scripts such as onBefore (on the assumption that there is no requirement to validate the import of reference fields). For example, `target.<field_name> = source.<field_name>.

Using multiple transform maps

Multiple transform maps can be applied to a single data source.

One import set row is created per transform map, which can cause a large number of temporary records to be generated.

**Note:** If you use multiple transform maps for the same import set, the transform creates multiple entries in the import set table.

Run multiple transforms off a single import set

Users can select multiple transform maps during data import.

The selected transform maps will be executed on the same import set in the order specified.
Multi-map transform

Transform map scripts

Transform Map scripts allow you to customize import operations using a robust programming interface to introduce advanced logic.

A transform map script executes as events occur while an import set is being transformed onto a ServiceNow table. Transform Map scripting is fully integrated into the ServiceNow scripting environment. There are two types of Transform Map scripts:

- Explicit Transform Map scripts, which explicitly define mapping relationships
- Transformation Event scripts, which modify the processing of events at different stages of a transformation

Transformation script variables

Multiple variables can be used to define explicit mapping relationships in a transform map script.

Variable name: source

Type: GlideRecord object

Description: Contains the import source record currently being transformed. Specify a specific field from the source record as an object property.

Example:

```javascript
var x = source.incident_state;
```
**Variable name: target**

**Type:** GlideRecord object

**Description:** Contains the import target record currently being inserted. Specify a specific field from the target record as an object property.

**Example:**

```java
target.incident_state = "active";
```

**Variable name: map**

**Type:** GlideRecord object

**Description:** Contains the transformation map record currently being used for the transformation process. Specify a specific field from the transform map record with one of these properties.

- `name`
- `sys_id`
- `source_table`
- `target_table`
- `order`

**Example:**

```java
var x = map.order;
```

**Variable name: log**

**Type:** Function

**Description:** Log information about the current import process. Each log level has its own method.

**Example:**

```java
log.info("This is an information message");
log.warn("This is a warning message");
log.error("This is an error message");
```

**Variable name: action**

**Type:** Function

**Description:** Specify the transformation action occurring on the target record. This value can be either “insert” or “update”.

**Example:**

```java
if(action == "insert"){
    ignore = true;
}
```

**Variable name: ignore**

**Type:** Boolean

**Description:** When set to true, skips or aborts the current import action. In onStart scripts, this variable aborts the entire transformation process. In onBefore scripts, this variable only skips the current row being transformed.
Example:

```java
if(source.u_user_name.nil()){
    ignore = true;
}
```

**Variable name: error**

**Type:** Boolean

**Description:** When set to true, aborts the current import action and logs an error message in the Import Set Log.

**Example:**

```java
if(source.name=="no_trantform"){
    error = true;
}
```

**Variable name: error_message**

**Type:** String (output message)

**Description:** When an error occurs, adds the specified error message to SOAP response.

**Example:**

```java
if(source.name=="no_trantform"){
    error = true;
    error_message = "Source is not intended for transformation";
}
```

**Variable name: status_message**

**Type:** String (output message)

**Description:** Adds the specified status message to SOAP response.

**Example:**

```java
if(action =="insert"){
    status_message = "Inserting record";
}
```

**Map with explicit transform map scripts**

Explicitly define mapping relationships in the Transform Map record itself.

An explicit Transform Map script explicitly defines mapping relationships in the Transform Map record itself. It runs after the source field values have been copied over to the target record, and before they are written to the database.

**CMDB software import facilitated by explicit mapping script**

An example demonstrating how explicit map scripting can be used to facilitate an import of software instances to the CMDB where it is necessary to have the count in the software packages table reflect the number of instances.

In the CMDB there exist tables for software packages and software instances. A software package refers to a one individual software title, such as Mozilla Firefox. A software instance refers to an individual instance of a software title such as Mozilla Firefox on Jared_T60_Laptop.
In more technical terms a software instance is a many-to-many relationship with a software package and a configuration item. This script imports software instances. In doing so it checks to see if a software package for the instance exists. If the software package doesn't exist then it is created and the sys_id for the newly created package is associated with the instance via the instance record's Software field.

```javascript
//First we will initialize some temporary variables, referencing values from the Import Set table source that will be used to reference software package records and create them if necessary.

var name= source.u_name;
var version = source.u_version;
var sid ="";

//Next we will perform a glide query on the software package table (Note: The target table for the import is software instances)
var sgr =new GlideRecord("cmdb_ci_spkg");

//Here we are building our query to search for software packages where the name and version of the package matches the name and version of the instance being imported
sgr.addQuery("name",name);
sgr.addQuery("version", version);
sgr.query();

//Now if a software package with the correct name and version are found then we record the sys_id of the package record otherwise we create the package and then record the sys_id
if(sgr.next()){
    sid = sgr.sys_id;}
else {// create it
    sgr.initialize();
    sgr.newRecord();
    sgr.name=name;
    sgr.version= version;
    sid = sgr.insert();

//Here we make an entry in System Import Set Log saying that we had to create a software package
log.info("Created new spkg: "+name+ " - "+ version);}

//Finally we set the reference field on our software instance record to the sys_id we have recorded for the software package. In doing so we are also relating the software package with the instance and so the count, which keeps track of the number of instances associated with a package, will automatically be incremented.
target.software= sid;
```

**Populating child tables by setting class names in an import to the CMDB**

An example demonstrating how to import servers into the configuration management database.

The destination table for the import is the cmdb_ci_servers table.

```javascript
var operating_system = source.u_operating_system.toString();

//This if statement uses JavaScript regular expressions to search the operating system
```

© 2021 ServiceNow, Inc. All rights reserved. ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
User import data sanitation

An example script demonstrating how to sanitize user data before import.

```javascript
//Note: The field names referenced from an import set are
//prefixed with an "u_", also note that it is necessary to use the java
//method
//toString() to so that we can use JavaScript functions to
//manipulate the data.
var name= source.u_name.toString();

//Use native JavaScript function split to create an array for each word in
//the name "splitting" it
//anywhere that there is a space
var split_names =name.split(" ");

//Find the number of of names (i.e., first and last name only, or first
//middle and last name, etc.)
var num_names = split_names.length;

// If there is only one name then map it to the last name field in the user
//table
if(num_names ==1){
target.last_name= split_names[0];}

//if there are two names then map the first one to first name and the last
//one to last name
if(num_names ==2){
target.first_name= split_names[0];
target.last_name= split_names[1];}

//if there are more than 3 names then all middle names get combined into one
//middle name this is done
//by shifting off the first name (array element 0 ) and mapping to first
//name and popping off the last
// name and returning it to the last name field
if(num_names >=3){
target.first_name= split_names.shift();
target.last_name= split_names.pop();
target.middle_name= split_names.join(" ");}
```

Map with transformation event scripts

Transformation events occur during the process of transforming an import set table onto a table.

These events modify the transformation behavior from any type of mapping specification. Transformation Event
scripts modify the processing of the events at various stages of the transformation.

For example, the processing of a mapping operation defined using the Mapping Assist Utility can be manipulated
using the event scripts. There are a number of import set JavaScript objects that are accessible during these events.
These objects represent tables or portions of tables. It is important to note that what these objects refer to varies
depending on the context of the event in which they are referenced.

The following is a table of all of the transform events and their contextual variables:
transform events and their contextual variables

<table>
<thead>
<tr>
<th>Event name</th>
<th>Event Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>onStart</td>
<td>When: The onStart event script is processed at the start of an import run, before any data rows are read.</td>
</tr>
</tbody>
</table>

**Import Set JS objects available to be referenced and their context in the onStart event**

<table>
<thead>
<tr>
<th>Import Set JS object</th>
<th>Type</th>
<th>Context in the onStart import set event</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>GlideRecord</td>
<td>The first row of the source table, there is no data yet since the row has not been read.</td>
</tr>
<tr>
<td>import_set</td>
<td>GlideRecord</td>
<td>The import set that is currently being transformed.</td>
</tr>
<tr>
<td>map</td>
<td>GlideTransformMap</td>
<td>Read-only information about the current transform map record.</td>
</tr>
<tr>
<td>log</td>
<td>Function</td>
<td>The log object for the current import run. For example, log.info(...), log.warn(...), log.error(...).</td>
</tr>
<tr>
<td>ignore</td>
<td>Boolean</td>
<td>When set to true, the entire transformation will be stopped and no further processing will occur.</td>
</tr>
<tr>
<td>error</td>
<td>Boolean</td>
<td>When set to true, has the same effect as the ignore flag of stopping the entire transformation, with an error message.</td>
</tr>
</tbody>
</table>

Example:

```javascript
var info = "Starting Import Set Transformation Mapping operation using Data source, " + map.table_source + " and Transform Map " + map.name + " on import set " + import_set.number;
log.info(info);
```
Event name | Event Parameters
---|---
oneComplete

When: The onComplete event script is processed at the end of an import run, after all data rows are read and transformed.

**Import Set JS objects available to be referenced and their context in the onComplete event**

<table>
<thead>
<tr>
<th>Import Set JS object</th>
<th>Type</th>
<th>Context in the onComplete import set event</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>GlideRecord</td>
<td>The last row of the source import set table.</td>
</tr>
<tr>
<td>target</td>
<td>GlideRecord</td>
<td>The last row of target table.</td>
</tr>
<tr>
<td>import_set</td>
<td>GlideRecord</td>
<td>The import set that is currently being transformed.</td>
</tr>
<tr>
<td>map</td>
<td>GlideTransformMap</td>
<td>Read-only information about the current transform map record.</td>
</tr>
<tr>
<td>log</td>
<td>Function</td>
<td>The log object for the current import run. For example, log.info(...), log.warn(...), log.error(...).</td>
</tr>
<tr>
<td>error</td>
<td>Boolean</td>
<td>When set to true, will mark the current import set status to error after it completes.</td>
</tr>
</tbody>
</table>

Example:

```javascript
// Create a myimport_completed event that can be reacted by an email notification or script action
// (there is already an import.finished event that the system will create at the end of an import)
var e = new GlideEvent("myimport_completed", import_set.sys_id, map.sys_id, "");
e.insert();
```
<table>
<thead>
<tr>
<th>Event name</th>
<th>Event Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>onBefore</td>
<td>When: The onBefore event script is processed at the start of a row transformation, before the source row is transformed into the target row.</td>
</tr>
</tbody>
</table>

**Import Set JS objects available to be referenced and their context in the onBefore event**

<table>
<thead>
<tr>
<th>Import Set JS object</th>
<th>Type</th>
<th>Context in the onBefore import set event</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>GlideRecord</td>
<td>The row of the source table that is currently being processed.</td>
</tr>
<tr>
<td>target</td>
<td>GlideRecord</td>
<td>The row of the target table that is currently being processed.</td>
</tr>
<tr>
<td>import_set</td>
<td>GlideRecord</td>
<td>The import set that is currently being transformed.</td>
</tr>
<tr>
<td>map</td>
<td>GlideTransformMap</td>
<td>Read-only information about the current transform map record.</td>
</tr>
<tr>
<td>log</td>
<td>Function</td>
<td>The log object for the current import run. For example, log.info(...), log.warn(...), log.error(...).</td>
</tr>
<tr>
<td>action</td>
<td>String</td>
<td>Action returns a value of either “insert” or “update” indicating whether the current target row is about to be created or updated.</td>
</tr>
<tr>
<td>ignore</td>
<td>Boolean</td>
<td>When set to true, the current row transformation will be skipped and the remaining rows will be processed.</td>
</tr>
<tr>
<td>Event name</td>
<td>Event Parameters</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>------------------</td>
<td></td>
</tr>
<tr>
<td>onAfter</td>
<td>When: The onAfter event script is processed at the end of a row transformation, after the source row has been transformed into the target row and saved.</td>
<td></td>
</tr>
</tbody>
</table>

**Import Set JS objects available to be referenced and their context in the onAfter event**

<table>
<thead>
<tr>
<th>Import Set JS object</th>
<th>Type</th>
<th>Context in the onAfter import set event</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>GlideRecord</td>
<td>The row of the source table that is currently being processed.</td>
</tr>
<tr>
<td>target</td>
<td>GlideRecord</td>
<td>The row of the target table that is currently being processed.</td>
</tr>
<tr>
<td>import_set</td>
<td>GlideRecord</td>
<td>The import set that is currently being transformed.</td>
</tr>
<tr>
<td>map</td>
<td>GlideTransformMap</td>
<td>Read-only information about the current transform map record.</td>
</tr>
<tr>
<td>log</td>
<td>Function</td>
<td>The log object for the current import run. For example, log.info(...), log.warn(...), log.error(...).</td>
</tr>
<tr>
<td>action</td>
<td>String</td>
<td>Action returns a value of either &quot;insert&quot; or &quot;update&quot; indicating whether the current target row was created or updated.</td>
</tr>
<tr>
<td>status_message</td>
<td>String</td>
<td>Defines a custom message to be sent in the &lt;status_message&gt; XML response.</td>
</tr>
<tr>
<td>error</td>
<td>Boolean</td>
<td>When set to true, will halt the entire import process.</td>
</tr>
</tbody>
</table>
**Event name** | **Event Parameters**
--- | ---
onForeignInsert | When: The onForeignInsert event script is processed at the start of the creation of a related, referenced record, before the record is created.

*Import Set JS objects available to be referenced and their context in the onForeignInsert event*

<table>
<thead>
<tr>
<th>Import Set JS object</th>
<th>Type</th>
<th>Context in the onForeignInsert import set event</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>GlideRecord</td>
<td>The row of the source table that is currently being processed.</td>
</tr>
<tr>
<td>target</td>
<td>GlideRecord</td>
<td>The row of the target table that is currently being processed.</td>
</tr>
<tr>
<td>map</td>
<td>GlideTransformMap</td>
<td>Read-only information about the current transform map record.</td>
</tr>
<tr>
<td>log</td>
<td>Function</td>
<td>The log object for the current import run. For example, log.info(...), log.warn(...), log.error(...).</td>
</tr>
<tr>
<td>action</td>
<td>String</td>
<td>Action returns a value of either “insert” or “update” indicating whether the current target row is about to be created or updated.</td>
</tr>
<tr>
<td>name</td>
<td>String</td>
<td>Evaluates to the field name of the target record for which a foreign record that is about to be created.</td>
</tr>
<tr>
<td>value</td>
<td>String</td>
<td>Evaluates to the display value from the source record.</td>
</tr>
<tr>
<td>Event name</td>
<td>Event Parameters</td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td>------------------</td>
<td></td>
</tr>
<tr>
<td>onChoiceCreate</td>
<td>When: The onChoiceCreate event script is processed at the start of a choice value creation, before the new choice value is created.</td>
<td></td>
</tr>
</tbody>
</table>

**Import Set JS objects available to be referenced and their context in the onChoiceCreate event**

<table>
<thead>
<tr>
<th>Import Set JS object</th>
<th>Type</th>
<th>Context in the onChoiceCreate import set event</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>GlideRecord</td>
<td>The row of the source table that is currently being processed.</td>
</tr>
<tr>
<td>target</td>
<td>GlideRecord</td>
<td>The row of the target table that is currently being processed.</td>
</tr>
<tr>
<td>map</td>
<td>GlideTransformMap</td>
<td>Read-only information about the current transform map record.</td>
</tr>
<tr>
<td>log</td>
<td>Function</td>
<td>The log object for the current import run. For example, log.info(...), log.warn(...), log.error(...).</td>
</tr>
<tr>
<td>action</td>
<td>String</td>
<td>Action returns a value of either &quot;insert&quot; or &quot;update&quot; indicating whether the current target row is about to be created or updated.</td>
</tr>
<tr>
<td>name</td>
<td>String</td>
<td>Evaluates to the field name of the target record for which a choice value is about to be created.</td>
</tr>
<tr>
<td>value</td>
<td>String</td>
<td>Evaluates to the display value from the source record for which a choice value is about to be created.</td>
</tr>
<tr>
<td>ignore</td>
<td>Boolean</td>
<td>When set to true, ignores the creation of a choice value.</td>
</tr>
<tr>
<td>error</td>
<td>Boolean</td>
<td>When set to true, rejects the entire transformation row, no data is saved for this row.</td>
</tr>
</tbody>
</table>

Example:

```
//Create an event
var e = new GlideEvent("myimport_ChoiceCreate", action, value, 
"");
```
### Event name

onReject

### Event Parameters

When: The onReject event script is processed during the occurrence of a foreign record or choice creation, and the foreign record or choice is rejected, the entire transformation row is not saved.

**Import Set JS objects available to be referenced and their context in the onError event**

<table>
<thead>
<tr>
<th>Import Set JS object</th>
<th>Type</th>
<th>Context in the onError import set event</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>GlideRecord</td>
<td>The row of the source table that is currently being processed.</td>
</tr>
<tr>
<td>target</td>
<td>GlideRecord</td>
<td>The row of the target table that is currently being processed.</td>
</tr>
<tr>
<td>map</td>
<td>GlideTransformMap</td>
<td>Read-only information about the current transform map record.</td>
</tr>
<tr>
<td>action</td>
<td>String</td>
<td>Action returns a value of either &quot;insert&quot; or &quot;update&quot; indicating whether the current target row is about to be created or updated.</td>
</tr>
<tr>
<td>log</td>
<td>Function</td>
<td>The log object for the current import run. For example, log.info(...), log.warn(...), log.error(...).</td>
</tr>
</tbody>
</table>

**Example:**

```javascript
//Create an event
var e = new GlideEvent("myimport_onReject", action, ",", ");
e.insert();
```
Robust Import Set Transformers

Use robust import set transformers instead of transform maps if you want to extract, transform, and load data to one or more target tables.

Robust import set transformers versus transform maps

Transform maps define the mapping from imported data stored in a staging table to a single target table in the Now Platform. Transform maps also insert data into target tables, performing both transform and processing functions. You can define multiple table mappings with multiple transform maps.

The Robust Transform Engine (RTE) and the robust import set transformer separate the transform and processing functions, providing a more flexible alternative to transform maps. The robust import set transformer allows you to extract data from a source table into an intermediary data structure. You can transform the data as desired and then load that data to one or more target tables. Records are processed as batches to enhance performance.

With transform maps, if you want data from the source table to go to three different target tables, you must create three separate transform maps. Each transform map parses the data separately, which results in three separate read operations. By contrast, the robust import set transformer requires only a single read operation to prepare the data for three target tables. The robust import set transformer is more efficient, especially when dealing with multiple target tables.

Extract Transform Load (ETL)

When you use the robust import set transformer, Extract Transform Load (ETL) functionality transfers imported data to target tables. You define how the data is extracted, transformed, and loaded to one or more target tables. You can use ETL definitions to do the following:

- Define entities (an abstraction similar to tables).
- Define entity fields (an abstraction similar to table fields).
- Define mapping between entities, and optionally designate whether a specific mapping should be ignored during data integration.
- Define entity field mappings.
- Define entity operations.

For procedures, see Create Extract Transform Load (ETL) definitions.

As of the Paris release, ETL definitions also support nested data structures such as the following when the Data source has JSON/XML payloads in a single column.

```json
{
  "records": [
    {
      "network": {
        "location": "San Diego",
        "computers": [
          {
            "id": "C100",
            "os": "Mac",
            "disks": [
              {
                "size": "200GB",
                "type": "SSD"
              },
              {
                "size": "1TB",
                "type": "Magnetic"
              }
            ]
          }
        ]
      }
    }
  ]
}
```
Create a robust import set transformer

Define how information is sent from the source table to target tables via a Robust Transform Engine (RTE).

Role required: importTransformer

1. Navigate to System Import Sets > Administration > Robust Import Set Transformers.
2. Click New.
3. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the robust import set transformer.</td>
</tr>
<tr>
<td>Source table</td>
<td>The source table for the robust import set transformer.</td>
</tr>
<tr>
<td>Robust transform engine</td>
<td>Enables you to select an ETL definition or CMDB definition. For procedures to define an RTE, see Create robust transform definitions.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the robust import set transformer.</td>
</tr>
<tr>
<td>Properties</td>
<td>Custom properties which can be used in processing the data.</td>
</tr>
<tr>
<td>Application</td>
<td>Application scope for this record.</td>
</tr>
<tr>
<td>Active</td>
<td>Selected if the robust import set transformer is currently active. Deselected if the robust import set transformer is not currently active.</td>
</tr>
<tr>
<td>Batch size</td>
<td>The number of items in each batch being transformed.</td>
</tr>
<tr>
<td>Verbose</td>
<td>Enables some transform logs that show how transform operations are applied to records.</td>
</tr>
</tbody>
</table>

4. Click Submit.

Create robust transform definitions

Specify your own Robust Transform Engine (RTE) to transfer data from a source table to a target table.
Role required: import_transformer

1. Navigate to System Import Sets > Administration > Robust Import Set Transformers.
2. Select an existing robust import set transformer, or click New to create a new robust import set transformer. For procedures, see Create a robust import set transformer.
3. At the Transformer Definition field, click the search icon.
4. On the Robust Transform Definitions window, click New.
5. On the Robust Transformer Definition pop-up, select ETL Definition.
6. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Selected if the robust transform engine is active. Deselected if the robust transform engine is not active.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the robust transform engine.</td>
</tr>
<tr>
<td>Application</td>
<td>Application scope for this record.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the robust transform engine.</td>
</tr>
</tbody>
</table>

7. Click Submit.

Create Extract Transform Load (ETL) definitions

Create ETL definitions to extract data from a source table, transform the data as desired, and load the data into a target table. ETL definitions also support nested data structures.

Role required: import_transformer

1. Navigate to System Import Sets > Administration > ETL Definitions.
2. Click New.
3. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the ETL definition.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the ETL definition.</td>
</tr>
<tr>
<td>Application</td>
<td>Application scope for this record.</td>
</tr>
<tr>
<td>Active</td>
<td>Selected if the ETL definition is active. Unselected if the ETL definition isn't active.</td>
</tr>
</tbody>
</table>

4. Click Submit.

Define ETL entities

Define the Extract Transform Load (ETL) entities used by the Robust Transform Engine.

Role required: import_transformer

1. Navigate to System Import Sets > Administration > ETL Definitions.
2. Select an ETL definition.
3. On the ETL Entities tab, click New.
4. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the ETL entity.</td>
</tr>
<tr>
<td>Table</td>
<td>Target table for the ETL entity.</td>
</tr>
</tbody>
</table>
Define ETL entity mappings
Map the source entity to a target entity.

Role required: import_transformer

You can optionally set the Ignore check box to exclude the entity mapping when performing data integrations using Robust Import Set Transformation (RTE).

1. Navigate to System Import Sets > Administration > ETL Definitions.
2. Select an ETL definition.
4. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the mapping.</td>
</tr>
<tr>
<td>Source Entity</td>
<td>Source entity for the mapping.</td>
</tr>
<tr>
<td>Target Entity</td>
<td>Target entity for the mapping.</td>
</tr>
<tr>
<td>Order</td>
<td>Order in which the mapping should be processed.</td>
</tr>
<tr>
<td>Is Conditional</td>
<td>Check box that designates that the mapping is conditional. Select the check box if the mapping is conditional and clear it if it is not.</td>
</tr>
<tr>
<td>Condition Script</td>
<td>Script that defines the conditions that must be met for the mapping.</td>
</tr>
<tr>
<td>Application</td>
<td>Application scope for this record.</td>
</tr>
<tr>
<td>Definition</td>
<td>Selected ETL entity that this mapping belongs to.</td>
</tr>
</tbody>
</table>
Create ETL entity field definitions
Define the entity fields mapped for Extract Transform Load (ETL) operations.

Role required: import_transformer

1. Navigate to **System Import Sets > Administration > ETL Definitions**.
2. Select an ETL definition.
3. On the ETL Entities tab, select an ETL entity.
4. On the ETL Entity fields tab, click **New**.
5. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the ETL Entity field definition.</td>
</tr>
<tr>
<td>Field/Path</td>
<td>Column name when the entity is Import or Target table, or a path when the field has nested structures.</td>
</tr>
<tr>
<td>Coercion action</td>
<td>What the system should do if a reference or choice could not be found. Available options are create, ignore, and reject.</td>
</tr>
<tr>
<td>Coalesce</td>
<td>Use this field to query the existing records.</td>
</tr>
<tr>
<td>Application</td>
<td>Application scope for this record.</td>
</tr>
<tr>
<td>Entity</td>
<td>Name of the robust transform engine entity.</td>
</tr>
<tr>
<td>Definition</td>
<td>Selected ETL entity that this field definition belongs to.</td>
</tr>
</tbody>
</table>

6. Click **Submit**.

Define Robust Transform Engine operations
Define the operations the Robust Transform Engine (RTE) should perform.

Role required: import_transformer
You should always perform operations on only one entry. Select all source and target fields from the same entity.

1. Navigate to **System Import Sets > Administration > ETL Definitions**.
2. Select an ETL definition.
3. On the ETL Entities tab, select an ETL entity.
4. On the RTE Entity Operations tab, click **New**.
5. Select the kind of operation you want to create.
6. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the operation.</td>
</tr>
<tr>
<td>Source Field</td>
<td>Input ETL field for the operation if the operation takes a single input.</td>
</tr>
<tr>
<td>Target Field</td>
<td>Output ETL field for the operation if the operation takes a single output.</td>
</tr>
<tr>
<td>Source Fields</td>
<td>Input ETL fields for the operation if the operation takes multiple inputs.</td>
</tr>
<tr>
<td>Target Fields</td>
<td>Output ETL fields for the operation if the operation takes multiple outputs.</td>
</tr>
<tr>
<td>Operation Group</td>
<td>Optional name to group related operations.</td>
</tr>
<tr>
<td>Overwrite Existing Value</td>
<td>If true, overwrites an existing non-empty value in the target fields.</td>
</tr>
<tr>
<td>Optional Joining String</td>
<td>Optional string to join values on.</td>
</tr>
<tr>
<td>Decimal Places</td>
<td>Optional number of decimal places to force output value to.</td>
</tr>
<tr>
<td>Remainder Target Field</td>
<td>Optional second target field to write the trimmed remainder of the source string after the first numeric value is removed.</td>
</tr>
<tr>
<td>Glide Matching Fields</td>
<td>Comma-delimited list of column names to use for lookup in the target table.</td>
</tr>
<tr>
<td>Target Table</td>
<td>Table to perform a lookup on.</td>
</tr>
<tr>
<td>Glide Target Fields</td>
<td>Comma-delimited list of columns to return from the target table.</td>
</tr>
<tr>
<td>Match Regular Expression</td>
<td>Matching regular expression for replace operations.</td>
</tr>
<tr>
<td>Replacement Regular Expression</td>
<td>Replacement string.</td>
</tr>
<tr>
<td>Use Unique Input Sets</td>
<td>If true, the operation processes only the unique set of inputs to the operation. Otherwise, the operation processes every record individually.</td>
</tr>
<tr>
<td>Literal Set Value</td>
<td>String value to set to target.</td>
</tr>
<tr>
<td>Splitting String</td>
<td>String to split the input value on.</td>
</tr>
<tr>
<td>Date Format</td>
<td>Date/time format expressed in simple Java format.</td>
</tr>
<tr>
<td>Order</td>
<td>Order in which the operation runs on the entity.</td>
</tr>
<tr>
<td>Script</td>
<td>Script that runs as part of the operation.</td>
</tr>
<tr>
<td>Is Conditional</td>
<td>Specifies whether to apply the operation if the specified conditions are met.</td>
</tr>
<tr>
<td>Conditional Fields</td>
<td>Fields to use in the condition.</td>
</tr>
</tbody>
</table>
Field | Description
--- | ---
Conditional Script | Condition specified as a string.
Application | Application scope for this record.
Operation Type | Operation type for this operation.
Entity | Entity this operation applies to.
Definition | Selected ETL entity definition that this entity and operation belong to.

7. Click **Submit**.

### Updating records using coalesce

The coalesce option allows you to update existing target table records when transforming import data.

The coalesce option on a field map allows you to specify if the selected **Target field** should be used to coalesce on when import set records are transformed. If the field map **Coalesce** checkbox is selected, when the import set row is transformed the instance checks for an existing record in the target table that has the same value in the **Target field** as the import set row **Source field**.

If an existing record with a matching value in the target table is found, that record is updated. If no matching record is found, then a new record is created in the target table.

**Note:** Choose fields in the target table to coalesce on only if those fields will have unique values. If more than one record in the target table matches the specified coalesce options, only the first matching record in the target table is updated.

### Coalesce options

There are several possible configurations you can use to coalesce data in import sets.

**No coalesce**

If no coalesce is defined, all imported rows are treated as new records. No existing records are updated.

**Single-field coalesce**

You can coalesce on a single field to update an existing record.

If a target table record exists with the same value in the coalesce field as the staging table record, the target table record is updated using the import set record values.

**Multiple-field coalesce**

You can coalesce on multiple fields to update an existing record.

If a target table record exists with the same values in all coalesce fields as the staging table record, the target table record is updated using the staging table record values. All coalesce field values between the target and staging tables must match to coalesce with multiple fields.
Conditional coalesce

You can use a script to determine if a staging table row should coalesce to a target record. Most conditional coalesce scripts are defined in the **Source script** field of a field map for the sys_id field. To update a target record using the staging table record values, the script must return the sys_id of the target table record.

**Example conditional coalesce scripts**

Review examples of conditional coalesce scripts.

**Updates only**

To only update records where a match is found, and skip records where a match is not found, specify a coalesce field and add the following script as an **onBefore** script to the transform map.

```javascript
if (action == 'insert')
    ignore = true;
```

**Conditional coalesce using dot-walking**

You can use dot-walked fields in a conditional coalesce script, such as to match the email address of a user when importing incident data.

In this example, this script is defined in the **Source script** of a field map for the Incident target table sys_id field.

```javascript
var now_GR = new GlideRecord('incident');
gr.addQuery('caller_id.email', source.u_email); //check if the incident caller's email matches the import row email value
gr.query();
if(gr.next())
{
    answer = gr.sys_id; //if a match exists, return the sys_id of the matching Incident record
}
else
{
    answer= -1;
}
```

**Conditional coalesce with an OR condition**

You can use a conditional coalesce script to match source and target records based on multiple field values. Unlike multiple-field coalesce where all coalesce fields must match, you can specify a script to only require one of the fields to match.

In this example, this script is defined in the **Source script** of a field map for the User target table sys_id field.

```javascript
var now_GR = new GlideRecord('sys_user');
var qc = gr.addQuery('email', source.u_email); //first check if the user's email matches
qc.addOrCondition('user_name', source.u_name); //alternatively, check if the username matches
```
```java
gr.query();
if(gr.next())
{
    answer = gr.sys_id; //if a match exists, return the sys_id of the matching User record
}
else
{
    answer = -1;
}
```

**Case-sensitive coalesce field values**

You can control if an import set will coalesce on matching values with different cases.

The field map **Coalesce case sensitive** field enables you to coalesce field values by case sensitivity.

By default, fields marked as **Coalesce** in the field map are used in a case insensitive lookup for existing records. If the **Coalesce case sensitive** check box is selected, the instance attempts to match coalesce field values by case. The target table record is updated only if the value in the target record and the import set staging record have the same value and case. Otherwise, a new record is created.

**Coalesce on empty fields**

You can control if an import set will coalesce on fields with no value.

The field map **Coalesce empty fields** field allows you to coalesce on fields with no value.

By default, fields marked as **Coalesce** in the field map cause the import set to check for a target record with a field value that matches the value from the import set staging record. When **Coalesce empty fields** is selected for that field map, an empty value in the target record and import set staging record counts as a match for the purpose of coalescing.

For example, the User transform map coalesces on the email field. With the **Coalesce empty fields** option selected, a source record containing an empty email address coalesces to a target record containing an empty email address.

**Standard import set tables**

Several Import Set tables are available by default.

**Notification**

A standard object for describing an external interface for a notification in the system, eg. alarms and alerts from monitoring systems. The default transform map for this object will create or update an incident record. The incoming notifications are coalesced into incidents based on the UUID field.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Data type</th>
</tr>
</thead>
<tbody>
<tr>
<td>uuid</td>
<td>The universally unique identification number or string that uniquely identifies this notification. It is marked as the coalescing value in the default transform map for the corresponding Incident and is mapped to the correlation_id field of Incident.</td>
<td>Character (40)</td>
</tr>
<tr>
<td>corrective_message</td>
<td>A free form string value that indicates the corrective or followup steps to be taken to address the issue identified in this notification. This field is not mapped by default.</td>
<td>Character (40)</td>
</tr>
<tr>
<td>duration</td>
<td>A string value representing the time value duration affecting the issue reported in this notification. Out of box, the duration field is not mapped. The format of the time is up to the calling program and must be mapped accordingly in the default map to be used.</td>
<td>Character (40)</td>
</tr>
<tr>
<td>expires_on</td>
<td>A string value representing the datetime value that the issue reported in this notification will expire. Out of box, the expires_on field is not mapped. The format of the time is up to the calling program and must be mapped accordingly in the default map to be used.</td>
<td>Character (40)</td>
</tr>
<tr>
<td>message</td>
<td>A string value describing the nature of the issue related to this notification. It should be a concise description and is mapped to the short_description field of the Incident.</td>
<td>Character (80)</td>
</tr>
<tr>
<td>comments</td>
<td>A string value containing additional comments related to this notification. The value is mapped to the comments field of the Incident.</td>
<td>Character (4000)</td>
</tr>
<tr>
<td>category</td>
<td>A string value categorising the nature of this notification. The value is mapped to the category field of the Incident, and therefore should be one of its valid values. If an existing value does not exist, the default behavior is to create a new category.</td>
<td>Character (40)</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Data type</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>assignment_group</td>
<td>A string value of the assignment group for this notification. The value is mapped to the assignment_group field of the Incident, and therefore should be one of its valid values. If an existing value does not exist, the default behavior is to create a new assignment group and set it for the resulting incident.</td>
<td>Character (40)</td>
</tr>
</tbody>
</table>
| severity      | A string representation of a numeric value that indicates the severity of the issue being reported in this notification. This field is mapped to the severity field on Incident. The out of box numeric values and their meanings are:  
  • 1 - High  
  • 2 - Medium  
  • 3 - Low | Character (40) |
| state         | A string that indicates the state of the issue being reported in this notification. This field is mapped to the incident_state field on Incident. The out of box values are:  
  • New  
  • Active  
  • Resolved  
  • Closed | Character (40) |
<p>| source        | A string value to indicate the source of the issue or the configuration item (by unique identifier eg IP address, host name etc) related to the issue in this notification. It’s mapped to the cmdb_ci field of Incident. | Character (40) |
| timestamp     | A string value representing the datetime value that marks the beginning of the issue reported in this notification. Out of box, the timestamp field is not mapped. The format of the time is up to the calling program and must be mapped accordingly in the default map to be used. | Character (40) |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Data type</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>A string value categorizing the type of issue related to this notification. Out of box, this field is not mapped to any field on Incident. Integrations using this Notification message may use this field to identify its source and trigger additional scripts.</td>
<td>Character (40)</td>
</tr>
</tbody>
</table>

**Computer**

A standard object for describing an external interface for a computer in the system. The default transform map will create/update a Computer (cmdb_ci_computer) or Server (cmdb_ci_server, cmdb_ci_win_server, cmdb_aix_server etc ..) based on the operating_system field value. The incoming computers are coalesced based on the serial_number field. Additionally, the transform script of the map will map to various extensions of the Computer (cmdb_ci_computer) based on the operating_system value being entered.

- UNIX Server (cmdb_ci_unix_server)
  - AIX
  - HP/UX
  - Solaris
  - AIX

- Windows Server (cmdb_ci_win_server)
  - Windows 2000 Server
  - Windows 2003 Server
  - Windows NT 4.0

- Server (cmdb_ci_server)
  - Any operating system that contains the word "Linux"

**imp_computer**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Data type</th>
</tr>
</thead>
<tbody>
<tr>
<td>serial_number</td>
<td>The unique identifier for this computer. It is marked as the coalescing value in the default transform map for the corresponding Computer and is mapped to the serial_number field of Computer (cmdb_ci_computer).</td>
<td>Character (40)</td>
</tr>
<tr>
<td>cpu_count</td>
<td>The number of CPUs that this computer has. It is mapped to the cpu_count field of the Computer (cmdb_ci_computer) table.</td>
<td>Character (40)</td>
</tr>
<tr>
<td>cpu_speed</td>
<td>The clock speed of the CPU in MHz. This field is mapped to the cpu_speed field of Computer (cmdb_ci_computer)</td>
<td>Character (40)</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Data type</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>cpu_type</td>
<td>Free form text describing the type of CPU. Example values are &quot;GenuineIntel&quot;, &quot;IBM&quot;, or &quot;Pentium 4&quot;. This field is mapped to the cpu_type field of Computer (cmdb_ci_computer)</td>
<td>Character (40)</td>
</tr>
<tr>
<td>disk_space</td>
<td>A numeric value describing the total disk space available to the computer in GB. This field is mapped to the disk_space field of Computer (cmdb_ci_computer)</td>
<td>Character (40)</td>
</tr>
<tr>
<td>manufacturer</td>
<td>A string name for the manufacturer of the computer. This field is mapped to the manufacturer field of Computer (cmdb_ci_computer) which is a reference to Company (core_company)</td>
<td>Character (40)</td>
</tr>
<tr>
<td>model_id</td>
<td>A string name for the model of the computer. This field is mapped to the model_id field of Computer (cmdb_ci_computer) which is a reference to Model Name (cmdb_model)</td>
<td>Character (40)</td>
</tr>
<tr>
<td>name</td>
<td>A string value representing the name of the Computer, usually a host name or IP/MAC address. It is mapped to the name field of Computer (cmdb_ci_computer)</td>
<td>Character (40)</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Data type</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>operating_system</td>
<td>A string value for the main operating system running on the computer. It is mapped to the os field of Computer (cmdb_ci_computer). Out of box values are:</td>
<td>Character (40)</td>
</tr>
<tr>
<td></td>
<td>• AIX</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• GNU/Linux</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• HP/UX</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Linux Fedora</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Linux Red Hat</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Linux SuSE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Mac OS 10 (OS/X)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Mac OS 8</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Mac OS 9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Mac OS/X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• OS/400</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Solaris</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SunOS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows 2000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows 2000 Advanced Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows 2000 Datacenter Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows 2000 Professional</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows 2000 Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows 2003 Datacenter</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows 2003 Enterprise</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows 2003 Standard</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows 2003 Web</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows 95</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows 98</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows ME</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows NT 4.0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows XP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows XP Home</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows XP Professional</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows 2000 Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows 2003 Enterprise</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows 2003 Enterprise</td>
<td></td>
</tr>
<tr>
<td>ram</td>
<td>A numeric value for the total number of memory installed on this computer in MB. This value is mapped to the ram field of Computer (cmdb_ci_computer)</td>
<td>Character (40)</td>
</tr>
</tbody>
</table>
User

A standard object for describing an external interface for a user in the system. The default transform map script sets the user_name field value to first_name.last_name if the web service's user_id field value is not supplied, otherwise, the user_id value is mapped directly to the user_name field in the User (sys_user) table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Data type</th>
</tr>
</thead>
<tbody>
<tr>
<td>email</td>
<td>A string value containing the user's email address. This value is mapped to the email field in User (sys_user) and is set as the coalesce value for the transform.</td>
<td>Character (40)</td>
</tr>
<tr>
<td>department</td>
<td>The department the user is in. This field is mapped to the department field in User (sys_user) which is a reference to the Department (cmn_department) table.</td>
<td>Character (40)</td>
</tr>
<tr>
<td>first_name</td>
<td>The first name of the user, mapped to the first_name field of the User (sys_user) table.</td>
<td>Character (40)</td>
</tr>
<tr>
<td>last_name</td>
<td>The last name of the user, mapped to the last_name field of the User (sys_user) table.</td>
<td>Character (40)</td>
</tr>
<tr>
<td>location</td>
<td>The location the user is in, mapped to the location field of the User (sys_user) table which is a reference field to Location (cmn_location)</td>
<td>Character (40)</td>
</tr>
<tr>
<td>phone</td>
<td>The phone number of the user, mapped to the phone (Business Phone) field of the User (sys_user) table.</td>
<td>Character (40)</td>
</tr>
<tr>
<td>user_id</td>
<td>This is the user identification, usually a login name, that maps to the user_name (User ID) field of the User (sys_user) table.</td>
<td>Character (40)</td>
</tr>
</tbody>
</table>

Location

A standard object for describing an external interface for a location in the system. The web service will create or modify records in the Location (cmn_location) table.
imp_location

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Data type</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>The name of the location, for example &quot;Headquarters&quot;, &quot;Sales office&quot; etc. This field is mapped to the name field of Location (cmn_location) and is part of the coalesce to search for an existing location.</td>
<td>Character (40)</td>
</tr>
<tr>
<td>street</td>
<td>The street address of the location, for example &quot;1234 ServiceNow way&quot; etc. This field is mapped to the street field of Location (cmn_location) and is part of the coalesce to search for an existing location.</td>
<td>Character (40)</td>
</tr>
<tr>
<td>city</td>
<td>The city of the location, for example &quot;San Diego&quot;, &quot;Madrid&quot; etc. This field is mapped to the city field of Location (cmn_location) and is part of the coalesce to search for an existing location.</td>
<td>Character (40)</td>
</tr>
<tr>
<td>state</td>
<td>The state of the location, for example &quot;California&quot;, &quot;Connecticut&quot; etc. This field is mapped to the city field of Location (cmn_location) and is part of the coalesce to search for an existing location.</td>
<td>Character (40)</td>
</tr>
<tr>
<td>zip</td>
<td>The zip code for the location, for example &quot;92130&quot;, &quot;10001&quot; etc. This field is mapped to the zip field of Location (cmn_location) and is part of the coalesce to search for an existing location.</td>
<td>Character (40)</td>
</tr>
<tr>
<td>country</td>
<td>The country for the location, for example &quot;USA&quot;, &quot;United Kingdom&quot; etc. This field is mapped to the country field of Location (cmn_location).</td>
<td>Character (40)</td>
</tr>
</tbody>
</table>

**Import sets maximum row size**

Rows imported using import sets must not exceed the maximum row size.

A single row in a database may not contain more than 8126 bytes of data. The size of each row is determined by the amount of content in all fields, as well as the character set for text fields. For example, a row with 10 text fields each containing 1000 characters using a French character set takes 15360 bytes.

Attempting to import more data to a single row than the maximum size causes the import to skip that row. Any rows that were skipped for this reason are listed in the import log.
**Importing data using import sets**

To import data define a data source and transform map, and run or schedule an import.

---

**Creating a data source**

Create a data source record to define what data an import set should import.

Depending on the type of data source you want to create, see the following topics for procedures.

*Create a File type data source*

Create a File type data source record to define what data an import set should import.

Role required: import_admin

For additional information, see [File type data sources](#).

1. Navigate to **System Import Sets > Administration > Data Sources**.
2. Click **New**.
3. Complete the form.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name for this data source.</td>
</tr>
<tr>
<td>Import set table label</td>
<td>A label for the import set staging table to use.</td>
</tr>
<tr>
<td>Import set table name</td>
<td>The uses the label you entered to construct a unique table name. This prevents namespace collision with an already existing table.</td>
</tr>
<tr>
<td>Type</td>
<td>File.</td>
</tr>
<tr>
<td>Format</td>
<td>Only the default XML-based file format (.xlsx) is supported, unless saved as &quot;Strict Open XML Document.&quot;</td>
</tr>
<tr>
<td>Zipped</td>
<td>Selected if the import file is compressed.</td>
</tr>
<tr>
<td>Use Batch Import</td>
<td>If selected, specifies that loading data should be batched when you click Load data or Test load 20 records.</td>
</tr>
<tr>
<td>Batch Size</td>
<td>Specifies how big the batches should be. Appears only when the Use Batch Import field is selected.</td>
</tr>
<tr>
<td>File retrieval method</td>
<td>The retrieval method for this file.</td>
</tr>
</tbody>
</table>

The glide.import_set_load_usebatch and glide.import_set_load_batch_size properties affect these fields. The priority order for the properties and fields are as follows: If the property is set, use the property value. If not, use the field value. If neither property is set, use the default batch size of 1000.

- For example, if `glide.import_set_load_usebatch = true` and `glide.import_set_load_batch_size = 200`, use 200 as the batch size, regardless of the field values.
- For example, if `glide.import_set_load_usebatch = true` and the `glide.import_set_load_batch_size` property is not set, use the default batch size of 1000.
- For example, if the `glide.import_set_load_usebatch` property is not set and the Use Batch Import field = true, use the Batch Size field value (or the default of 1000 if the Batch Size field value is not set)
- For example, if the `glide.import_set_load_usebatch` property = false and the Use Batch Import field = true, do not use batch import, since the property is set to false.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File path</td>
<td>The path to the file to import. You can include a system property value in this field using the format <code>${system.property.name}</code>. When the connection is made, the variable is replaced with the value of the specified property.</td>
</tr>
<tr>
<td><strong>Note:</strong> For files retrieved using HTTP or HTTPS, the <code>glide.ds.file.http.variable_replacement</code> property must be true to use system property expansion.</td>
<td></td>
</tr>
<tr>
<td>For example, you can specify the file <em>path</em> value <code>/countries.csv?key=${datasource.apikey}</code>. When the connection is made, the value of the <code>datasource.apikey</code> system property is passed as the value for the <strong>key</strong> parameter.</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> For HTTP and HTTPS protocols, the file path is automatically URL encoded. Do not specify a URL-encoded file path when using either of these protocols.</td>
<td></td>
</tr>
<tr>
<td>CSV delimiter</td>
<td>The delimiter character for the CSV file.</td>
</tr>
<tr>
<td>Parsing script</td>
<td>The script used to parse a single line of input. As you type the script, script auto-complete presents the choices available to you. For more information, see File type data sources.</td>
</tr>
<tr>
<td>Sheet number</td>
<td>The Excel sheet number to load data.</td>
</tr>
<tr>
<td>Header row</td>
<td>The Excel sheet number to load the column labels.</td>
</tr>
<tr>
<td>Path for each row</td>
<td>The path expression used to select JSON objects, which will become rows in the import set table. The path should be <code>/</code> for JSON objects.</td>
</tr>
<tr>
<td>Discard Arrays</td>
<td>Selected to discard JSON arrays as a value. Unselected to serialize JSON arrays as a value.</td>
</tr>
<tr>
<td>Expand node children</td>
<td>Selected if child elements of the XML node or JSON object should be converted into additional columns. Unselected if the parent column value should be an XML or JSON fragment. For JSON, note that selecting this option expands objects only, not arrays. For nested array support, see Importing JSON files.</td>
</tr>
<tr>
<td>Data in single column</td>
<td>Selected to store data in a single column.</td>
</tr>
<tr>
<td>Xpath for each row</td>
<td>XPath expression that selects the nodes which become rows in the import table. The children of the selected nodes will become the columns in the rows.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SCP authentication method</td>
<td>Choice to authenticate with a username and password or with a public key.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You cannot authenticate to data sources with a public-private key pair. Use a username and password authentication instead.</td>
</tr>
<tr>
<td>Server</td>
<td>Name of the server from which the tables will be imported.</td>
</tr>
<tr>
<td>Port</td>
<td>Port to use to connect to the specified server. This field appears if you select HTTP or HTTPS as the file retrieval method.</td>
</tr>
<tr>
<td>Username</td>
<td>User name for authentication on the JDBC server.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for authentication on the JDBC server.</td>
</tr>
<tr>
<td>Private keyfile</td>
<td>Keyfile when using legacy SCP public-private keyfiles.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td></td>
<td>• You cannot authenticate to data sources with a public-private key pair. Use username and password authentication instead.</td>
</tr>
<tr>
<td></td>
<td>• Do not use this legacy option. Although it is available for use, it is not supported.</td>
</tr>
<tr>
<td>System keystore</td>
<td>Selected to validate the certificate from the FTPS server against all saved certificates. This certificate may be any type supported by the instance. If not selected, the instance uses the Java default certificate to validate the FTPS server. This field is available only for data sources with a file retrieval method value of FTPS. All FTPS file retrieval methods are supported, including Auth TLS, Auth SSL, Implicit SSL, and Implicit TLS.</td>
</tr>
</tbody>
</table>

4. **Click** Submit.

Define a transform map for the new data source and run an import.

*Create a JDBC type data source*

Create a **JDBC** type data source record to define what data an import set should import.

Role required: import_admin

For additional information, see JDBC type data source.

1. Navigate to **System Import Sets > Administration > Data Sources**.
2. Click **New**.
3. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name for this data source.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Import set table label</td>
<td>A label for the import set staging table to use.</td>
</tr>
<tr>
<td>Import set table name</td>
<td>The uses the label you entered to construct a unique table name. This prevents namespace collision with an already existing table.</td>
</tr>
<tr>
<td>Type</td>
<td>JDBC.</td>
</tr>
<tr>
<td>Use MID Server</td>
<td>MID Server to use to connect to this data source.</td>
</tr>
<tr>
<td>Format</td>
<td>Select one of the following formats: MySQL, Oracle, or SQLServer.</td>
</tr>
<tr>
<td>Instance name</td>
<td>Used to support dynamic port connectivity with SQL Server. To ensure connectivity, provide the instance name for a SQL Server that receives a new port number dynamically after each reboot. This field only appears when SQLServer is selected as a data source format.</td>
</tr>
<tr>
<td>Database name</td>
<td>Name of the database instance.</td>
</tr>
<tr>
<td>Database port</td>
<td>Port number for the database. Leave this field empty when using dynamic port connectivity with SQL Server.</td>
</tr>
<tr>
<td>Use Batch Import</td>
<td>If selected, specifies that loading data should be batched when you click Load data or Test load 20 records.</td>
</tr>
<tr>
<td>Batch Size</td>
<td>Specifies how big the batches should be. Appears only when the Use Batch Import field is selected.</td>
</tr>
</tbody>
</table>

The glide.import_set_load_usebatch and glide.import_set_load_batch_size properties affects these fields. The priority order for the properties and fields are as follows: If the property is set, use the property value. If not, use the field value. If neither property is set, use the default batch size of 1000.

- For example, if
  glide.import_set_load_usebatch = true and glide.import_set_load_batch_size = 200, use 200 as the batch size, regardless of the field values.
- For example, if
  glide.import_set_load_usebatch = true and the glide.import_set_load_batch_size property is not set, use the default batch size of 1000.
- For example, if the glide.import_set_load_usebatch property is not set and the Use Batch Import field = true, use the Batch Size field value (or the default of 1000 if the Batch Size field value is not set)
- For example, if the glide.import_set_load_usebatch property = false and the Use Batch Import field = true, do not use batch import, since the property is set to false.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use integrated authentication</td>
<td>Selected to allow the JDBC connection to use the ID of the user configured for the Windows MID Server service for SQL Server authentication. For additional details, see JDBC type data source.</td>
</tr>
<tr>
<td>Username</td>
<td>User name for authentication on the JDBC server.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for authentication on the JDBC server.</td>
</tr>
<tr>
<td>Server</td>
<td>Name of the server from which the tables will be imported.</td>
</tr>
<tr>
<td>Query</td>
<td>Type of query to run: All rows from Table or Specific SQL. If you select to run a SQL statement, the SQL statement field appears.</td>
</tr>
<tr>
<td>Query timeout</td>
<td>Number of seconds the JDBC driver will wait for a query (SELECT) to complete. Zero (0) means no timeout. If timeout is exceeded, the integration considers the JDBC result inaccessible and places it in an error state.</td>
</tr>
<tr>
<td>Connection timeout</td>
<td>Number of seconds before MID Server connection cache pool closes and removes it from the pool. Zero (0) means no timeout.</td>
</tr>
<tr>
<td>Table name</td>
<td>Name of the table from which the data is being exported.</td>
</tr>
<tr>
<td>SQL statement</td>
<td>SQL statement to extract the desired data from the database.</td>
</tr>
<tr>
<td>Use last run datetime</td>
<td>Controls the amount of data that is retrieved from a database during an import run. If unselected, then all rows in the table specified are imported, every time. You might want to use this setting if this is a one-time import, or if all the data in the target table is new. If selected, two additional fields appear, enabling you to select a datetime value to limit imported data to delta values only.</td>
</tr>
<tr>
<td>Last run datetime</td>
<td>The datetime value in this field is automatically populated from the database field you select below and represents the latest value from the previous run. This value acts as a dynamic filter to restrict the number of records retrieved to those records that have changed since the data source's last runtime.</td>
</tr>
<tr>
<td>Last run database field</td>
<td>Field name from the source table that will be used as the filter in the next run. This value may need to be case sensitive, depending on the target database type.</td>
</tr>
<tr>
<td>Additional Database Parameters</td>
<td>Optional parameters to add to the end of the URL generated for this data source. Semicolon-separated list of parameters. You may need to configure the form to view this field.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

Define a transform map for the new data source and run an import.

Create an **LDAP type data source**

Create an **LDAP** type data source record to define what data an import set should import.

Role required: **import_admin**
For additional information, see LDAP type data source.

1. Navigate to **System Import Sets > Administration > Data Sources.**
2. Click **New.**
3. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name for this data source.</td>
</tr>
<tr>
<td>Import set table label</td>
<td>A label for the import set staging table to use.</td>
</tr>
<tr>
<td>Import set table name</td>
<td>The uses the label you entered to construct a unique table name. This prevents namespace collision with an already existing table.</td>
</tr>
<tr>
<td>Type</td>
<td>LDAP.</td>
</tr>
<tr>
<td>LDAP target</td>
<td>Target selected from the list of your LDAP OU definitions.</td>
</tr>
<tr>
<td>Use Batch Import</td>
<td>If selected, specifies that loading data should be batched when you click <strong>Load data</strong> or <strong>Test load 20 records</strong>.</td>
</tr>
<tr>
<td>Batch Size</td>
<td>Specifies how big the batches should be. Appears only when the <strong>Use Batch Import</strong> field is selected.</td>
</tr>
</tbody>
</table>

The `glide.import_set_load_usebatch` and `glide.import_set_load_batch_size` properties affect these fields. The priority order for the properties and fields are as follows: If the property is set, use the property value. If not, use the field value. If neither property is set, use the default batch size of 1000.

- For example, if `glide.import_set_load_usebatch = true` and `glide.import_set_load_batch_size = 200`, use 200 as the batch size, regardless of the field values.
- For example, if `glide.import_set_load_usebatch = true` and the `glide.import_set_load_batch_size` property is not set, use the default batch size of 1000.
- For example, if the `glide.import_set_load_usebatch` property is not set and the **Use Batch Import** field = `true`, use the **Batch Size** field value (or the default of 1000 if the **Batch Size** field value is not set)
- For example, if the `glide.import_set_load_usebatch` property = false and the **Use Batch Import** field = `true`, do not use batch import, since the property is set to false.

4. Click **Submit.**

Define a transform map for the new data source and run an import.
Create an OIDC type data source

Create an **OIDC** type data source record to define what data an import set should import.

Role required: import_admin

1. Navigate to **System Import Sets > Administration > Data Sources**.
2. Click **New**.
3. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name for this data source.</td>
</tr>
<tr>
<td>Import set table label</td>
<td>A label for the import set staging table to use.</td>
</tr>
<tr>
<td>Import set table name</td>
<td>The uses the label you entered to construct a unique table name. This prevents namespace collision with an already existing table.</td>
</tr>
<tr>
<td>Type</td>
<td><strong>OIDC</strong>.</td>
</tr>
<tr>
<td>Use Batch Import</td>
<td>If selected, specifies that loading data should be batched when you click <strong>Load data</strong> or <strong>Test load 20 records</strong>.</td>
</tr>
<tr>
<td>Batch Size</td>
<td>Specifies how big the batches should be. Appears only when the <strong>Use Batch Import</strong> field is selected.</td>
</tr>
</tbody>
</table>

The **glide.import_set_load_usebatch** and **glide.import_set_load_batch_size** properties affect these fields. The priority order for the properties and fields are as follows: If the property is set, use the property value. If not, use the field value. If neither property is set, use the default batch size of 1000.

- For example, if
  - **glide.import_set_load_usebatch = true** and
  - **glide.import_set_load_batch_size = 200**,
  - use 200 as the batch size, regardless of the field values.

- For example, if
  - **glide.import_set_load_usebatch = true** and
  - the **glide.import_set_load_batch_size** property is not set,
  - use the default batch size of 1000.

- For example, if the **glide.import_set_load_usebatch** property is not set and the **Use Batch Import** field = **true**,
  - use the **Batch Size** field value (or the default of 1000 if the **Batch Size** field value is not set)

- For example, if the **glide.import_set_load_usebatch** property = **false** and the **Use Batch Import** field = **true**,
  - do not use batch import, since the property is set to false.

| Format | Defaults to **None** and can't be changed. |

4. Click **Submit**.

Define a transform map for the new data source and run an import.
Create a REST (IntegrationHub) type data source
Create a REST (IntegrationHub) type data source record to define what data an import set should import from a REST API.

Roles required: import_admin and action_designer

1. Navigate to System Import Sets > Administration > Data Sources.
2. Click New.
3. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name for this data source.</td>
</tr>
<tr>
<td>Import set table label</td>
<td>A label for the import set staging table to use.</td>
</tr>
<tr>
<td>Import set table name</td>
<td>The uses the label you entered to construct a unique table name. This prevents namespace collision with an already existing table.</td>
</tr>
<tr>
<td>Type</td>
<td>REST (IntegrationHub).</td>
</tr>
<tr>
<td>Format</td>
<td>One of the following formats: Custom (Parse by Script), JSON, or XML.</td>
</tr>
<tr>
<td>Use Batch Import</td>
<td>If selected, specifies that loading data should be batched when you click Load data or Test load 20 records.</td>
</tr>
</tbody>
</table>
| Batch Size             | Specifies how big the batches should be. Appears only when the Use Batch Import field is selected. The glide.import_set_load_usebatch and glide.import_set_load_batch_size properties affects these fields. The priority order for the properties and fields are as follows: If the property is set, use the property value. If not, use the field value. If neither property is set, use the default batch size of 1000.

- For example, if glide.import_set_load_usebatch $= true$ and glide.import_set_load_batch_size $= 200$, use 200 as the batch size, regardless of the field values.
- For example, if glide.import_set_load_usebatch $= true$ and the glide.import_set_load_batch_size property is not set, use the default batch size of 1000.
- For example, if the glide.import_set_load_usebatch property is not set and the Use Batch Import field $= true$, use the Batch Size field value (or the default of 1000 if the Batch Size field value is not set)
- For example, if the glide.import_set_load_usebatch property $= false$ and the Use Batch Import field $= true$, do not use batch import, since the property is set to false.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request action</td>
<td>Data source request action that will be invoked to get data. You can choose only published request actions. Click the link in the dialog box below to create/configure a new Data Source request action in IntegrationHub. After the request action is published in IntegrationHub, you can choose it as a Request action in the Data Source record. For more information, see Define action properties.</td>
</tr>
<tr>
<td>Support pagination</td>
<td>Selected to enable pagination for the request action. Pagination helps you reduce processing overhead by processing a specified number of records at a time, instead of processing all records at once.</td>
</tr>
<tr>
<td>Limit</td>
<td>Maximum number of records per page. For example, to process 50 records at a time, enter a Limit of 50.</td>
</tr>
<tr>
<td>Offset</td>
<td>The initial offset used for pagination. The offset is the starting record number. For example, to process 50 records at a time, starting with the first record, enter a Limit of 50 and an Offset of 0.</td>
</tr>
<tr>
<td>Parsing script</td>
<td>Type the script used to parse a single line of input. Three parameters are available in this function:</td>
</tr>
<tr>
<td></td>
<td>• line: the current line to be parsed by the script</td>
</tr>
<tr>
<td></td>
<td>• lineNumber: the line number of the current line in the entire response payload</td>
</tr>
<tr>
<td></td>
<td>• result: output result</td>
</tr>
<tr>
<td>Path for each row</td>
<td>The path expression used to select JSON objects, which will become rows in the import set table. The path should be // for JSON objects.</td>
</tr>
<tr>
<td>Discard Arrays</td>
<td>Selected to discard JSON arrays as a value. Unselected to serialize JSON arrays as a value.</td>
</tr>
<tr>
<td>Expand node children</td>
<td>Selected if child elements of the XML node or JSON object should be converted into additional columns. Unselected if the parent column value should be an XML or JSON fragment. For JSON, note that selecting this option expands objects only, not arrays. For nested array support, see Importing JSON files.</td>
</tr>
<tr>
<td>Data in single column</td>
<td>Selected to store data in a single column.</td>
</tr>
<tr>
<td>Xpath for each row</td>
<td>XPath expression that selects the nodes which become rows in the import table. The children of the selected nodes will become the columns in the rows.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

Define a transform map for the new data source and run an import.

Define action properties

Create and configure a Data Source request action in IntegrationHub. After the request action is published in IntegrationHub, you can choose it as a **Request action** in the Data Source record.

Role required: import_admin

1. Navigate to **System Import Sets > Administration > Data Sources**.
2. Select **New**.
3. Select a Type of REST (IntegrationHub).
4. Click the link under Request action.
5. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the request action.</td>
</tr>
<tr>
<td>Accessible From</td>
<td>Scope from which the request action is accessible.</td>
</tr>
<tr>
<td>Category</td>
<td>Category of the request action.</td>
</tr>
<tr>
<td>Protection</td>
<td>Specifies whether the request action is read-only.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the request action.</td>
</tr>
<tr>
<td>Application</td>
<td>Scope of the application.</td>
</tr>
<tr>
<td>In-Flow Annotation</td>
<td>Text you want to appear under the Action title on the Data Source Request Action page.</td>
</tr>
</tbody>
</table>

6. Click Submit.
7. The Data Source Request Action page appears with the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limit</td>
<td>Limit set by the user in the REST (IntegrationHub) data source record. If the REST API supports pagination and Support pagination is selected in the Data Source record, you must supply this input to your REST step.</td>
</tr>
<tr>
<td>Offset</td>
<td>Offset set by user in the REST (IntegrationHub) data source record. If the REST API supports pagination and Support pagination is selected in the Data Source record, you must supply this input to your REST step.</td>
</tr>
<tr>
<td>Last Success Import Time</td>
<td>Last time data was successfully imported. A numeric value representing the number of milliseconds since January 1, 1970, 00:00:00 GMT. The data source populates this value. If the REST API supports queries based on time, you must supply this input to your REST step.</td>
</tr>
<tr>
<td>Import Start Time</td>
<td>Time the import is actually started. A numeric value representing the number of milliseconds since January 1, 1970, 00:00:00 GMT. The data source populates this value. If the REST API supports queries based on time, you must supply this input to your REST step.</td>
</tr>
</tbody>
</table>

8. If desired, you can add a Script step to validate or modify action inputs, set default values, or build request payloads before executing the REST step.
   a) Select Data Source Request from the Action Outline.
   b) Select Enable Processing Script.
   c) Select Script step from the Action Outline.
   d) Configure the Script step as described in Script step.

10. Configure the REST step as described in REST step.
11. Choose from the following:
   • Click **Properties** to return to the Action Properties window.
   • Click **Test** to test the request action before publishing it.
   • Click **Executions** to view the history of executions of the request action.
   • Click **Save** to save the request action.
   • Click **Publish** to publish the request action and make it available for use.

Create a Custom (Load by Script) type data source

Create a **Custom (Load by Script)** type data source record to define what data an import set should import.

Role required: import_admin

For additional information, see **Custom (Load by Script) type data source**.

1. Navigate to **System Import Sets > Administration > Data Sources**.
2. Click **New**.
3. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name for this data source.</td>
</tr>
<tr>
<td>Import set table label</td>
<td>A label for the import set staging table to use.</td>
</tr>
<tr>
<td>Import set table name</td>
<td>The label you entered to construct a unique table name. This prevents namespace collision with an already existing table.</td>
</tr>
<tr>
<td>Type</td>
<td><strong>Custom (Load by Script)</strong>.</td>
</tr>
<tr>
<td>Use Batch Import</td>
<td>If selected, specifies that loading data should be batched when you click <strong>Load data</strong> or <strong>Test load 20 records</strong>.</td>
</tr>
</tbody>
</table>
### Field Description

**Batch Size**

Specifies how big the batches should be. Appears only when the **Use Batch Import** field is selected.

The `glide.import_set_load_usebatch` and `glide.import_set_load_batch_size` properties affect these fields. The priority order for the properties and fields are as follows: If the property is set, use the property value. If not, use the field value. If neither property is set, use the default batch size of 1000.

- For example, if `glide.import_set_load_usebatch = true` and `glide.import_set_load_batch_size = 200`, use 200 as the batch size, regardless of the field values.
- For example, if `glide.import_set_load_usebatch = true` and the `glide.import_set_load_batch_size` property is not set, use the default batch size of 1000.
- For example, if the `glide.import_set_load_usebatch` property is not set and the **Use Batch Import** field = true, use the **Batch Size** field value (or the default of 1000 if the **Batch Size** field value is not set).
- For example, if the `glide.import_set_load_usebatch` property = false and the **Use Batch Import** field = true, do not use batch import, since the property is set to false.

### Data Loader

Script used to load data. For more information, see Custom (Load by Script) type data source.

4. Click **Submit**.

Define a transform map for the new data source and run an import.

**Data source fields**

In addition to common fields, other fields appear on the data source form, depending on the value of the **Type** field.

**Common data source fields**

These fields are common to all data sources.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name for this data source.</td>
</tr>
<tr>
<td>Import set table label</td>
<td>A label for the import set staging table to use.</td>
</tr>
<tr>
<td>Import set table name</td>
<td>The uses the label you entered to construct a unique table name. This prevents namespace collision with an already existing table.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Type</td>
<td>The type of data you are importing:</td>
</tr>
<tr>
<td></td>
<td>• From a remote <strong>File</strong></td>
</tr>
<tr>
<td></td>
<td>• From a <strong>JDBC</strong> database</td>
</tr>
<tr>
<td></td>
<td>• Using <strong>LDAP</strong></td>
</tr>
<tr>
<td></td>
<td>• Using <strong>OIDC</strong></td>
</tr>
<tr>
<td></td>
<td>• Using <strong>REST</strong> to import data through the IntegrationHub</td>
</tr>
<tr>
<td></td>
<td>• From a <strong>Data Stream</strong> action through the</td>
</tr>
<tr>
<td></td>
<td>• Using a <strong>Custom</strong> script</td>
</tr>
<tr>
<td>Use Batch Import</td>
<td>If selected, specifies that loading data should be batched when you click <strong>Load data</strong> or <strong>Test load 20 records</strong>.</td>
</tr>
<tr>
<td>Batch Size</td>
<td>Specifies how big the batches should be. Appears only when the <strong>Use Batch Import</strong> field is selected.</td>
</tr>
<tr>
<td></td>
<td>The <strong>glide.import_set_load_usebatch</strong> and <strong>glide.import_set_load_batch_size</strong> properties affects these fields. The priority order for the properties and fields are as follows: If the property is set, use the property value. If not, use the field value. If neither property is set, use the default batch size of 1000.</td>
</tr>
<tr>
<td></td>
<td>• For example, if <strong>glide.import_set_load_usebatch = true</strong> and <strong>glide.import_set_load_batch_size = 200</strong>, use 200 as the batch size, regardless of the field values.</td>
</tr>
<tr>
<td></td>
<td>• For example, if <strong>glide.import_set_load_usebatch = true</strong> and the <strong>glide.import_set_load_batch_size</strong> property is not set, use the default batch size of 1000.</td>
</tr>
<tr>
<td></td>
<td>• For example, if the <strong>glide.import_set_load_usebatch</strong> property is not set and the <strong>Use Batch Import</strong> field = true, use the <strong>Batch Size</strong> field value (or the default of 1000 if the <strong>Batch Size</strong> field value is not set)</td>
</tr>
<tr>
<td></td>
<td>• For example, if the <strong>glide.import_set_load_usebatch</strong> property = false and the <strong>Use Batch Import</strong> field = true, do not use batch import, since the property is set to false.</td>
</tr>
<tr>
<td>Application</td>
<td>Application scope for this record.</td>
</tr>
</tbody>
</table>

**File type data source fields**

These additional fields appear on the data source form when the **Type** field value is **File**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>Only the default XML-based file format (.xlsx) is supported, unless saved as &quot;Strict Open XML Document.&quot;</td>
</tr>
<tr>
<td>Zipped</td>
<td>Selected if the import file is compressed.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>File retrieval method</td>
<td>The retrieval method for this file.</td>
</tr>
<tr>
<td>File path</td>
<td>The path to the file to import. You can include a system property value in this field using the format <code>${system.property.name}</code>. When the connection is made, the variable is replaced with the value of the specified property.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For files retrieved using HTTP or HTTPS, the glide.ds.file.http.variable_replacement property must be true to use system property expansion.</td>
</tr>
<tr>
<td></td>
<td>For example, you can specify the file path value /countries.csv?key=${datasource.apikey}. When the connection is made, the value of the datasource.apikey system property is passed as the value for the key parameter.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For HTTP and HTTPS protocols, the file path is automatically URL encoded. Do not specify a URL-encoded file path when using either of these protocols.</td>
</tr>
<tr>
<td>CSV delimiter</td>
<td>The delimiter character for the CSV file.</td>
</tr>
<tr>
<td>Parsing script</td>
<td>The script used to parse a single line of input. As you type the script, script auto-complete presents the choices available to you. For more information, see File type data sources.</td>
</tr>
<tr>
<td>Sheet number</td>
<td>The Excel sheet number to load data.</td>
</tr>
<tr>
<td>Header row</td>
<td>The Excel sheet number to load the column labels.</td>
</tr>
<tr>
<td>Path for each row</td>
<td>The path expression used to select JSON objects, which will become rows in the import set table. The path should be / / for JSON objects.</td>
</tr>
<tr>
<td>Discard Arrays</td>
<td>Selected to discard JSON arrays as a value. Unselected to serialize JSON arrays as a value.</td>
</tr>
<tr>
<td>Expand node children</td>
<td>Selected if child elements of the XML node or JSON object should be converted into additional columns. Unselected if the parent column value should be an XML or JSON fragment. For JSON, note that selecting this option expands objects only, not arrays. For nested array support, see Importing JSON files.</td>
</tr>
<tr>
<td>Data in single column</td>
<td>Selected to store data in a single column.</td>
</tr>
<tr>
<td>Xpath for each row</td>
<td>XPath expression that selects the nodes which become rows in the import table. The children of the selected nodes will become the columns in the rows.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| SCP authentication method | Choice to authenticate with a username and password or with a public key.  

**Note:** You cannot authenticate to data sources with a public-private key pair. Use a username and password authentication instead.                                                                                                                                                                                                                                    |
| Server                | Name of the server from which the tables will be imported.                                                                                                                                                                                                                                                                                                                                                         |
| Port                  | Port to use to connect to the specified server. This field appears if you select HTTP or HTTPS as the file retrieval method.                                                                                                                                                                                                                                                                                     |
| Username              | User name for authentication on the JDBC server.                                                                                                                                                                                                                                                                                                                                                                  |
| Password              | Password for authentication on the JDBC server.                                                                                                                                                                                                                                                                                                                                                                   |
| Private keyfile       | Keyfile when using legacy SCP public-private keyfiles.  

**Note:**  
- You cannot authenticate to data sources with a public-private key pair. Use username and password authentication instead.  
- Do not use this legacy option. Although it is available for use, it is not supported.                                                                                                                                                                                                                                                                     |
| System keystore       | Selected to validate the certificate from the FTPS server against all saved certificates. This certificate may be any type supported by the instance. If not selected, the instance uses the Java default certificate to validate the FTPS server. This field is available only for data sources with a **File retrieval method** value of FTPS. All FTPS file retrieval methods are supported, including Auth TLS, Auth SSL, Implicit SSL, and Implicit TLS.                                                                               |

**JDBC type data source fields**

These additional fields appear on the data source form when the **Type** field value is **JDBC**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use MID Server</td>
<td>MID Server to use to connect to this data source.</td>
</tr>
<tr>
<td>Format</td>
<td>One of the following formats: MySQL, Oracle, or SQLServer.</td>
</tr>
<tr>
<td>Instance name</td>
<td>Used to support dynamic port connectivity with SQL Server. To ensure connectivity, provide the instance name for a SQL Server that receives a new port number dynamically after each reboot. This field only appears when <strong>SQLServer</strong> is selected as a data source format.</td>
</tr>
<tr>
<td>Database name</td>
<td>Name of the database instance.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Database port</td>
<td>Port number for the database. Leave this field empty when using dynamic port connectivity with SQL Server.</td>
</tr>
<tr>
<td>Use integrated authentication</td>
<td>Selected to allow the JDBC connection to use the ID of the user configured for the Windows MID Server service for SQL Server authentication. For additional details, see JDBC type data source.</td>
</tr>
<tr>
<td>Username</td>
<td>User name for authentication on the JDBC server.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for authentication on the JDBC server.</td>
</tr>
<tr>
<td>Server</td>
<td>Name of the server from which the tables will be imported.</td>
</tr>
<tr>
<td>Query</td>
<td>Type of query to run: <strong>All rows from Table</strong> or <strong>Specific SQL</strong> If you select to run a SQL statement, the SQL statement field appears.</td>
</tr>
<tr>
<td>Query timeout</td>
<td>Number of seconds the JDBC driver will wait for a query (SELECT) to complete. Zero (0) means no timeout. If timeout is exceeded, the integration considers the JDBC result inaccessible and places it in an error state.</td>
</tr>
<tr>
<td>Connection timeout</td>
<td>Number of seconds before MID Server connection cache pool closes and removes it from the pool. Zero (0) means no timeout.</td>
</tr>
<tr>
<td>Table name</td>
<td>Name of the table from which the data is being exported.</td>
</tr>
<tr>
<td>SQL statement</td>
<td>SQL statement to extract the desired data from the database.</td>
</tr>
<tr>
<td>Use last run datetime</td>
<td>Controls the amount of data that is retrieved from a database during an import run. If unselected, then all rows in the table specified are imported, every time. You might want to use this setting if this is a one-time import, or if all the data in the target table is new. If selected, two additional fields appear, enabling you to select a datetime value to limit imported data to delta values only.</td>
</tr>
<tr>
<td>Last run datetime</td>
<td>The datetime value in this field is automatically populated from the database field you select below and represents the latest value from the previous run. This value acts as a dynamic filter to restrict the number of records retrieved to those records that have changed since the data source’s last runtime.</td>
</tr>
<tr>
<td>Last run database field</td>
<td>Field name from the source table that will be used as the filter in the next run. This value may need to be case sensitive, depending on the target database type.</td>
</tr>
<tr>
<td>Additional Database Parameters</td>
<td>Optional parameters to add to the end of the URL generated for this data source. Semicolon-separated list of parameters. You may need to configure the form to view this field.</td>
</tr>
</tbody>
</table>

**LDAP type data source field**

This additional field appears on the data source form when the **Type** field value is **LDAP**.
### LDAP target

Target selected from the list of your LDAP OU definitions.

### OIDC type data source field

This additional field appears on the data source form when the `Type` field value is **OIDC**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>Defaults to <strong>None</strong> and can’t be changed.</td>
</tr>
</tbody>
</table>

### REST (IntegrationHub) type data source fields

These additional fields appear on the data source form when the `Type` field value is **REST (IntegrationHub)**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>One of the following formats: Custom (Parse by Script), JSON, or XML.</td>
</tr>
<tr>
<td>Request action</td>
<td>Data source request action that will be invoked to get data. You can choose only published request actions. Click the link in the dialog box below to create/configure a new Data Source request action in . After the request action is published in , you can choose it as a <strong>Request action</strong> in the Data Source record. For more information, see Define action properties.</td>
</tr>
<tr>
<td>Support pagination</td>
<td>Selected to enable pagination for the request action. Pagination helps you reduce processing overhead by processing a specified number of records at a time, instead of processing all records at once.</td>
</tr>
<tr>
<td>Limit</td>
<td>Maximum number of records per page. For example, to process 50 records at a time, enter a <strong>Limit</strong> of 50.</td>
</tr>
<tr>
<td>Offset</td>
<td>The initial offset used for pagination. The offset is the starting record number. For example, to process 50 records at a time, starting with the first record, enter a <strong>Limit</strong> of 50 and an <strong>Offset</strong> of 0.</td>
</tr>
<tr>
<td>Parsing script</td>
<td>The script used to parse a single line of input. As you type the script, script auto-complete presents the choices available to you. For more information, see File type data sources.</td>
</tr>
<tr>
<td>Path for each row</td>
<td>The path expression used to select JSON objects, which will become rows in the import set table. The path should be <code>/</code> for JSON objects.</td>
</tr>
<tr>
<td>Discard Arrays</td>
<td>Selected to discard JSON arrays as a value. Unselected to serialize JSON arrays as a value.</td>
</tr>
</tbody>
</table>
### Field

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expand node children</td>
<td>Selected if child elements of the XML node or JSON object should be converted into additional columns. Unselected if the parent column value should be an XML or JSON fragment. For JSON, note that selecting this option expands objects only, not arrays. For nested array support, see Importing JSON files.</td>
</tr>
<tr>
<td>Data in single column</td>
<td>Selected to store data in a single column.</td>
</tr>
<tr>
<td>Xpath for each row</td>
<td>XPath expression that selects the nodes which become rows in the import table. The children of the selected nodes will become the columns in the rows.</td>
</tr>
</tbody>
</table>

### Data Stream (IntegrationHub) type data source fields

These additional fields appear on the data source form when the Type field value is Data Stream (IntegrationHub).

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Data Stream () type data source.</td>
</tr>
<tr>
<td>Data Stream action</td>
<td>• Selected to use an existing published Data Stream action from .</td>
</tr>
<tr>
<td></td>
<td>• Selected for one of the following reasons:</td>
</tr>
<tr>
<td></td>
<td>• If you select a published Data Stream action, click this button to open the Data Stream action in .</td>
</tr>
<tr>
<td></td>
<td>• If you don't select a Data Stream action, click this button to create and publish a new Data Stream action in .</td>
</tr>
<tr>
<td>Note:</td>
<td>Data Stream actions require a subscription for production use.</td>
</tr>
<tr>
<td>Data in single column</td>
<td>Selected to store data in a single column.</td>
</tr>
<tr>
<td>Data Stream action inputs</td>
<td>Additional fields may appear, based on the inputs defined in the Data Stream action.</td>
</tr>
</tbody>
</table>

### Custom (Load by Script) type data source field

This additional field appears on the data source form when the Type field value is Custom (Load by Script).
Create a transform map

Every import operation to a production table requires at least one transform map associated with an import set.

Role required: import_transformer, import_admin, or admin

The transform map specifies the data relationships between the import set and the target table. For every transformation, you must either create a new transform map or select an existing one.

1. Navigate to System Import Sets > Create Transform Map.
2. Complete the form.

Table transform map fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>User-friendly label to identify the transform map.</td>
</tr>
<tr>
<td>Source table</td>
<td>Import table containing the raw import set data. An import table is any table</td>
</tr>
<tr>
<td></td>
<td>that extends the Import Set Row [sys_import_set_row] table. You can select</td>
</tr>
<tr>
<td></td>
<td>only tables within the currently selected application scope.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box to make the transform map available for use.</td>
</tr>
<tr>
<td>Run business rules</td>
<td>Check box to run business rules, workflows, approval engines, auditing, and</td>
</tr>
<tr>
<td></td>
<td>field normalization while the transformation inserts or updates data into</td>
</tr>
<tr>
<td></td>
<td>the target table. Clearing this check box runs GlideRecord.setWorkflow()</td>
</tr>
<tr>
<td></td>
<td>with a value of false.</td>
</tr>
<tr>
<td>Enforce mandatory fields</td>
<td>Selects whether to enforce mandatory fields on the target table:</td>
</tr>
<tr>
<td></td>
<td>• No: Do not enforce mandatory fields.</td>
</tr>
<tr>
<td></td>
<td>• Only Mapped Fields: Enforce mandatory mapped fields only.</td>
</tr>
<tr>
<td></td>
<td>• All Fields: Enforce all mandatory fields.</td>
</tr>
<tr>
<td>Copy empty fields</td>
<td>Check box to copy empty field values and override existing target field</td>
</tr>
<tr>
<td></td>
<td>values.</td>
</tr>
<tr>
<td>Create new record on empty</td>
<td>Check box to create a new record when all coalesce fields are empty, instead</td>
</tr>
<tr>
<td>coalesce fields</td>
<td>of ignoring the record or overwriting an existing record.</td>
</tr>
<tr>
<td></td>
<td>If Coalesce empty fields is selected for any field in the record, the record</td>
</tr>
<tr>
<td></td>
<td>is coalesced.</td>
</tr>
<tr>
<td>Application</td>
<td>Application scope: global or per application.</td>
</tr>
<tr>
<td>Created</td>
<td>Transform map creation date (populated automatically).</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target table</td>
<td>The table in which you want the transformed data to be inserted. You can select only tables within the currently selected application scope or the global scope, or tables that grant write access to other applications.</td>
</tr>
<tr>
<td>Order</td>
<td>Order in which to apply transform maps if more than one map fits the conditions. The system runs transform maps from lowest to highest Order.</td>
</tr>
<tr>
<td>Run script</td>
<td>Check box to define a script that transforms field values in the source table to the target table.</td>
</tr>
<tr>
<td>Script</td>
<td>Transform map script that transforms field values in the source table to the target table. The system runs the transform map script in addition to any field maps.</td>
</tr>
</tbody>
</table>

**Important:** The string **NULL** is a reserved word. It should not be used as a field value in import set transform maps or anywhere in the **First name** or **Last name** fields. The reserved word is **NULL** in all capital letters. A field with the value **null** or **null**, for example, is acceptable. **NULL** should be used only to clear out a particular field.

## Mapping options

You can map fields in a number of ways depending on the circumstances of the import and whether data must be transformed prior to loading onto a production table.

It is also important to note that any given import operation may require taking advantage of multiple mapping methods, and these methods can be readily used in conjunction with one another.

### Automatic Mapping Utility

The simplest mapping method is where all of the field names of the import sets match the names of the fields on the production tables onto which the data will be transformed. In this case, simply click **Auto map matching fields** in the related list in the Table Transform Map form and confirm proper matching. If there are any discrepancies in terms of how fields were automatically matched, use the mapping assist utility to correct them. When all fields are matched properly, click the **Transform** related link to begin transforming data onto the destination table.

### Mapping Assist Utility

The mapping assist utility provides a visually intuitive environment for specifying mapping between import set fields and production table fields. The mapping assist utility makes it possible to map a single source field (field on an import set table) to multiple destination fields (fields on a production table).
Mapping assist

Changing the Date Format

If the date format of the source field does not match the format of the target field, you can set a date format mapping to transform dates from one format to another. For example, this mapping specifies that the date format of the CSV source file uses the **MM-dd-yyyy** format.
Field map date format

### Field map date format options

Date format options include:

#### Mapping Options

<table>
<thead>
<tr>
<th>Date Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dd-MM-yyyy</td>
<td>Day-month-year</td>
</tr>
<tr>
<td>dd-MM-yyyy hh:mm:ss</td>
<td>Day-month-year hours-minutes-seconds</td>
</tr>
<tr>
<td>dd-MM-yyyy hh:mm:ss z</td>
<td>Day-month-year hours-minutes-seconds timezone</td>
</tr>
<tr>
<td>MM-dd-yyyy</td>
<td>Month-day-year</td>
</tr>
<tr>
<td>MM-dd-yyyy hh:mm:ss</td>
<td>Month-day-year hours-minutes-seconds</td>
</tr>
<tr>
<td>MM-dd-yyyy hh:mm:ss z</td>
<td>Month-day-year hours-minutes-seconds timezone</td>
</tr>
</tbody>
</table>
You can specify a custom date format using **HH** to denote 24 hour time. Converting from a 24 hour to 12 hour date format may cause times from 12:00 to 12:59 to be formatted as 00:00.

### Mapping to a Duration Field

ServiceNow duration fields use a special data type that lists the number of milliseconds the duration value is. To map import data to a duration field use one of the following methods to transform source values into a duration.

- Calculate the duration from a start and end date
- Convert an existing duration value into a ServiceNow duration value

### Calculating a Duration Value from a Start and End Date

If the import source has a start and end date, you can calculate a duration with JavaScript.

1. Navigate to **System Import Sets > Transform Maps**.
2. Select the transform map you want to calculate a duration value. For example, the Notification transform map that imports into the Incident table.
3. Select the **Run script** check box.
4. Enter JavaScript to transform the start and end dates into a duration. See the sample script.
5. Click **Update**.

This sample script transforms the source.u_start and source.u_end fields to a duration value in the target.duration field. Change the field names to match your source and target fields as needed.

```javascript
target.duration = gs.dateDiff(source.u_start.getDisplayValue(), source.u_end.getDisplayValue(), false);
```

### Convert a Duration Value into a ServiceNow Duration Value

If the import source already contains a start date and a duration value, you can convert the existing duration into a ServiceNow duration. For example, you might have an Excel data source that lists a duration in seconds. ServiceNow expects durations to have millisecond values.

1. Navigate to **System Import Sets > Transform Maps**.
2. Select a transform map.
   - For example, the Notification transform map that imports into the Incident table.
3. Select the **Run script** check box.
4. Enter JavaScript to convert existing duration values into a ServiceNow duration values. See the sample script.

<table>
<thead>
<tr>
<th>Date Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>yyyy-dd-MM</td>
<td>Year-day-month</td>
</tr>
<tr>
<td>yyyy-MM-dd</td>
<td>Year-month-day</td>
</tr>
<tr>
<td>yyyy-MM-dd hh:mm:ss</td>
<td>Year-month-day hours-minutes-seconds</td>
</tr>
</tbody>
</table>
5. Click **Update**.

This sample script converts a duration in seconds (from the `source.u_duration` field) to a duration in milliseconds (in the `target.duration` field). Change the field names to match your source and target fields, as needed.

```javascript
//Transform the value in source.u_duration from seconds to milliseconds
target.duration.setDateNumericValue(source.u_duration * 1000);
```

This sample script converts a duration already in milliseconds (from the `source.u_duration` field) to a ServiceNow duration (in the `target.duration` field). Change the field names to match your source and target fields, as needed.

```javascript
//Transform the value in source.u_duration to ServiceNow format
target.duration.setDateNumericValue(source.u_duration);
```

**Using a Script to Calculate a Source Value**

You may want to use a source script instead of the **Source field** when:

- The source value is not in the format for the mapped target value.
- You want to look up a value before mapping to the target field.
- The source value must be computed from multiple fields.
- You need to create a compounded or calculated coalesce value in the target field.

For example, this example source script computes the value of the `user_name` field when it is blank in the source.

```javascript
if (source.user_id.nil()) {
  answer = source.first_name + "," + source.last_name;
} else answer = source.user_name;
```
A source script expects the calculated value to be set in the global variable `answer`.

**Mapping Binary or BLOB Fields**

ServiceNow uses a special process to import binary and binary large object (BLOB) data from JDBC data sources. All binary data is automatically converted into a record in the Attachment [sys_attachment] table before the transformation occurs. The import set table only stores the attachment record's sys_id value in the import table field instead of the actual binary value. For example, suppose you use a JDBC data source to import data from a CA Service Desk system, which stores each record's key value as binary data. When you import the Service Desk key values into a ServiceNow table, the ServiceNow field only contains a sys_id reference to the corresponding binary data in the Attachment Record [sys_attachment] table rather than the actual binary data.

To have a transform map access the attachment, use the `GlideRecord` API in an `onAfter` script. The script needs to run in an `onAfter` event because the `target.sys_id` object is only available after the data is placed in the import set table. For example, to map the resulting attachment to the target transform record, you can use the following script.

```javascript
var agr = new GlideRecord("sys_attachment");
agr.addQuery("sys_id", source.u_blob_field);
// the source field needs to be mapped to the source that is the BLOB
agr.query();
if(agr.next()) {
    agr.table_name = "cmdb_ci"; // the target table of the transform map
    agr.table_sys_id = target.sys_id; // the target record
    agr.content_type = source.u_contenttype;
    // the content type string if available,
    // this becomes the mime encoding when clicking an attachment link
    agr.update(); // finally, move/re-attach the attachment to the target
row }
```

If you are mapping directly to the `db_image` table, run the following `onAfter` script to display the image:

```javascript
var strTemp = source.u_file_name;
var fType = strTemp.substr(-3);
var iCont = "";
if(fType == 'jpg') {
    iCont = 'jpeg';
}
else {
    iCont = fType;
}
var agr = new GlideRecord("sys_attachment");
agr.addQuery("sys_id", source.u_blob_field);
agr.query();
if(agr.next()) {
    agr.table_name = "ZZ_YYdb_image";
    agr.table_sys_id = target.sys_id;
    agr.content_type = 'image/' + iCont;
    agr.file_name = 'image';
    agr.update(); }
```

**Create a field map**

Field maps establish a relationship between a field in an import set table and a field in the target table.

Role required: import_transformer, import_admin, or admin

The field map determines what values from the source table the transformation adds to the target table.

1. Navigate to System Import Sets > Transform Maps.
2. Open a transform map.
3. In the **Field Maps** related list, click **New**.
4. Complete the form.

### Field map fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Map</td>
<td>Transform map that uses this field mapping (populated automatically).</td>
</tr>
<tr>
<td>Source table</td>
<td>Table from which the raw import set data is loaded (the source for the transformation). Populated automatically from the transform map.</td>
</tr>
<tr>
<td>Source field</td>
<td>Field on the source table to be transformed. Can be blank if the Source table contains only raw data.</td>
</tr>
<tr>
<td>Choice action</td>
<td>Specifies the action to take if the import set contains a reference or choice value other than those available. Appears if the target field is a choice list or reference field.</td>
</tr>
<tr>
<td></td>
<td>• <strong>create</strong>: Create a new choice or record in the reference table.</td>
</tr>
<tr>
<td></td>
<td>• <strong>ignore</strong>: Ignore the new value from the source table.</td>
</tr>
<tr>
<td></td>
<td>• <strong>reject</strong>: Skip the entire row (record) containing the new value and continue to the next row.</td>
</tr>
<tr>
<td>Date format</td>
<td>Date format of the source field. Appears if the target field is a Date or Date/Time field.</td>
</tr>
<tr>
<td>Note: To learn more about allowable date formats, see Global date and time field format.</td>
<td></td>
</tr>
<tr>
<td>Use source script</td>
<td>Check box to use a script instead of the Source field.</td>
</tr>
<tr>
<td>Application</td>
<td>Application scope: global or per application.</td>
</tr>
<tr>
<td>Target table</td>
<td>Table in which the transformed data is inserted. You can select only tables within the currently selected application scope or the global scope, or tables that grant write access to other applications.</td>
</tr>
<tr>
<td>Target field</td>
<td>Field in the target table where the value from the source field is stored.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Referenced field value name</td>
<td>When the target field is a reference field, the transform map needs a way to match incoming source values to existing records in the reference field's source table. Since most imports do not provide a 32-character sys_id value, you must specify a column from the reference field's source table that contains values that match the incoming source values. When there is a matching record, the transform map stores the sys_id of the matching record in the target field. If there is no matching record, the transform map creates a new record in the reference field's table and stores the sys_id of the new record in the target field. If you leave this field blank, the transform map looks for matching values from the display value column of the reference field table. For example, suppose you are importing incident records and the incoming data lists user IDs for the Assigned to field. If you leave Referenced value field name blank, the transform map searches for matching values in the User table's display value column: name. By setting the Referenced value field name to the user_name column, you can match the user ID values to the appropriate user records.</td>
</tr>
<tr>
<td>Coalesce</td>
<td>Configuring a target field to coalesce causes the import set to treat the field as a unique key. When selected, the import set application attempts to match source values to records with values from an existing record. If a match is found, the transform map updates the record instead of creating a new record. When false, the import set application always creates new records for each transformation. If multiple fields are set to coalesce, all coalesce values must match an existing record. If two fields are set for coalescing and a matching value is found for one of the coalescing fields but not on the other, a new record is inserted. You must create an index on the target table if none of the coalesce fields are indexed. Indexing can improve performance for read and write operations. If one or more coalesce fields already has an index, you do not need to create an additional index. After setting the Coalesce value for all fields on the target table, use the Index Coalesce Fields related link to create an index. Before creating the index, ensure that the Coalesce value is set correctly for all fields on the target table to avoid creating unnecessary indexes for the same target table. The index needs to be concatenated; meaning all fields specified to be coalesced, need to be in the same index. The correct setup is for one index to include all fields being coalesced.</td>
</tr>
</tbody>
</table>
### Field map script variables

Several predefined variables are available in the **Source script** field.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>GlideRecord</td>
<td>The record from the source table that is currently being processed.</td>
</tr>
<tr>
<td>target</td>
<td>GlideRecord</td>
<td>The record from the target table that is currently being processed.</td>
</tr>
<tr>
<td>answer</td>
<td>String</td>
<td>The field value to set in the target record.</td>
</tr>
<tr>
<td>map</td>
<td>GlideTransformMap</td>
<td>Read-only information about the current transform map record.</td>
</tr>
<tr>
<td>log</td>
<td>Function</td>
<td>The log object for the current import run. Use this object to log messages such as <code>log.info(&quot;&lt;Message&gt;&quot;)</code> or <code>log.warn(&quot;&lt;Message&gt;&quot;)</code>. This object logs to the import log for standard import sets, or other log locations as required, such as for web service imports.</td>
</tr>
<tr>
<td>action</td>
<td>String</td>
<td>Contains either the value <strong>insert</strong> or <strong>update</strong>, depending on whether the current target row will be created or updated.</td>
</tr>
</tbody>
</table>

**Note:** The `action` variable is available only when the **Coalesce** field is **false**.
Run an import

You can manually run an import to immediately import data.

1. From a Transform Map, click Transform.

   When the import is done, you’ll see a link to go straight to the target table containing your imported records. The amount of time that it takes to run an import varies depending on the number of record to be imported and may take as long as several hours for very large import operations (tens of thousands of records).

2. [optional] Click on the link View the imported data to see the loaded import set table.

3. [optional] Click on the link Create transform map to create a new transform map to transform the data in the import set table to its target table.

4. [optional] Click on the link Run import to execute an existing transform map for the loaded data.

Three things to note at this point:

- The spreadsheet was imported, and a new table was created to hold the data.
- Within that table, the imported records are designated with their own "Set" value.
- A new module was created in the System Import Sets application for the new table.

Importing date/time values

Considerations when importing data containing date/time values.

- The field containing the date/time value should be a Date/Time type field in the target table.
- The user performing the import should have their timezone (in the Time zone [time_zone] field in the User [sys_user] record for that user) set to match the timezone of the date/time values in the import file.

To set the user timezone, do the following.

1. Click the user drop-down in the banner and select Profile.

2. Change the Time zone field value to the timezone of the date/time values in the import file and click Update.

Review the import set

After an import set completes, you can review the completed import and clean up import set tables. Even if no errors were reported by the progress indicator, review how your data was imported into the new import set.

1. Click View imported data.

   There are several fields that will be visible in the table that were not part of the original data source, these are system rows can be used to facilitate scripted import operations.

2. Review the data.

3. Return to the previous page.

Create a transform map to associate with this import set.

Viewing the import log

The import log is where you can find information about the internal processing that occurs during an import operation.

The log includes information generated by the system during the every step of the import operation from initialization of the import set table from a data source to transformation onto a target table. It is also possible to customize log outputs during the transformation by using log.info, log.warn, log.error statements.
Import Log

The import history gives status information about individual import operations.

Note: Functionality described here requires the Admin role.

Run import utility

The Run Import utility is used to run an import operation using an existing Transform Map and Import Set table.
Error Codes are related to a transformation. Not all errors produce error codes. If an error code does exist, it is in the [sys_import_set_row_error] table error code field.

**Error Codes**

- **100** Reference field value rejected.
- **200** Choice field value rejected.
- **300** List reference field rejected.
- **800** Invalid target record or field.
- **900** Transform script error.

**Schedule a data import**

Scheduled imports make it possible to specify that certain import operations should occur at some regular interval.

Role required: import_scheduler, import_admin, or admin

1. Navigate to **System Import Sets > Administration > Scheduled Imports**.
2. Complete the form.
Scheduled Data Import form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name for the scheduled data import.</td>
</tr>
<tr>
<td>Data source</td>
<td>Data source record that defines the data to import. If you select a remote data source, it is refreshed via the remote connection before the import begins.</td>
</tr>
<tr>
<td>Run as</td>
<td>Name of a user whose credentials the import job uses. If you do not specify a value, the import job runs as the guest user.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box to activate the scheduled import.</td>
</tr>
<tr>
<td>Run</td>
<td>Frequency at which you want to run the import.</td>
</tr>
<tr>
<td>Day</td>
<td>Day on which to run the import. Visible only if you set Run to Weekly or Monthly.</td>
</tr>
<tr>
<td>Time</td>
<td>Time you want the import to begin. Do not schedule multiple imports at the same time. Running multiple imports at the same time may negatively impact performance or cause an instance outage.</td>
</tr>
<tr>
<td>Repeat interval</td>
<td>Period that must elapse before the import is repeated. Visible only if you set Run to Periodically.</td>
</tr>
<tr>
<td>Starting</td>
<td>Date on which the import should begin (selected using the calendar icon). Visible only if you set Run to Periodically.</td>
</tr>
<tr>
<td>Parent</td>
<td>The parent import set to which this import set belongs, and after which this import should run. Visible only if you set Run to After Parent Runs.</td>
</tr>
<tr>
<td>Conditional</td>
<td>Check box to specify a script that defines the conditions that must evaluate to true before the import runs.</td>
</tr>
<tr>
<td>Condition</td>
<td>Script that evaluates whether an import should run. Visible only if you select the Conditional check box.</td>
</tr>
<tr>
<td>Concurrent Import</td>
<td>Check box to run a concurrent import. A concurrent import splits the data into multiple import sets and runs the import sets concurrently to reduce processing time for large data sets.</td>
</tr>
</tbody>
</table>

**Note:** A concurrent import does not transform data in a predictable order. If order matters, do not run a concurrent import.

For more information, see Concurrent imports.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partition Method</td>
<td>Method used to allocate each data set record to an import set:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Round Robin</strong>: The system sets partitions automatically. Assume 20 records and 4 import sets. The system allocates record 1 to import set 1, record 2 to import set 2, record 3 to import set 3, and record 4 to import set 4. The system then allocates record 5 to import set 1, record 6 to import set 2, record 7 to import set 3, and record 8 to import set 4. This continues until all records are assigned to import sets. When allocation is finished, import set 1 contains records 1, 5, 9, 13, 17. Import set 2 contains records 2, 6, 10, 14, 18. Import set 3 contains records 3, 7, 11, 15, and 19. Import set 4 contains records 4, 8, 12, 16, and 20.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Custom Script</strong>: Sets the partitions with a Partition Script you provide.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Custom size</strong>: Sets the partition size to the Partition Size specified. Once the system processes the first partition, the data from that partition can be transformed, even though the other partitions have not finished processing.</td>
</tr>
<tr>
<td>Partition Script</td>
<td>Script to return a partition key. The system ensures that data set rows with the same partition key go to the same import set. Visible only if you set <strong>Partition Method</strong> to Custom Script.</td>
</tr>
<tr>
<td>Partition Size</td>
<td>The number of records in each partition. Visible only if you select a <strong>Partition Method</strong> of Custom size.</td>
</tr>
<tr>
<td>Execute pre-import script</td>
<td>Check box to specify a script to run before the import is performed.</td>
</tr>
<tr>
<td>Pre script</td>
<td>Script to run before the data is imported. Visible only if you select the Execute pre-import script check box.</td>
</tr>
<tr>
<td>Execute post-import script</td>
<td>Check box to specify a script to run after the import is performed.</td>
</tr>
<tr>
<td>Post script</td>
<td>Script to run after the import is performed. Visible only if you select the Execute post-import script check box.</td>
</tr>
</tbody>
</table>

**Note:** For concurrent imports, the script runs after the last Import Set Transformer job completes.
3. Click **Submit**.
To stop an import that is taking too much time, navigate to **System Import Sets > Advanced > Progress**.
   a. Open the Progress Worker that must be canceled.
   b. In the Related Links, click **Cancel job**.

**Scheduled data import scripting options**
Multiple JavaScript objects are available in the Scheduled Data Import **Pre script** and **Post script** fields.

### Data import scripting options

<table>
<thead>
<tr>
<th>Object</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>cancel</td>
<td>Set this object to <strong>true</strong> to stop the import action.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Use the <strong>Pre script</strong> field to evaluate the conditions of the import and determine whether to cancel the import process. To cancel the import process, use the following call:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>```</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cancel = true;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>```</td>
<td></td>
</tr>
<tr>
<td>import_set</td>
<td>Get the GlideRecord object for the new import set. This variable allows you to query the following columns from the sys_import_set table:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• sys_id</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• state</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• table_name</td>
<td></td>
</tr>
<tr>
<td>data_source</td>
<td>GlideRecord of the data source to be used for the scheduled import.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Typically, you define the data source with the Scheduled Data Import record. If you want to access this data source or modify the data source in certain conditions, you can use the following.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>```</td>
<td></td>
</tr>
<tr>
<td></td>
<td>data_source.import_set_table_name = 'new_set_from_scheduler';</td>
<td></td>
</tr>
<tr>
<td></td>
<td>data_source.update();</td>
<td></td>
</tr>
</tbody>
</table>

**Monitor concurrent import sets**

Check the status of import sets and import set jobs, resume or reprocess import sets, and view transform history.

When a scheduled concurrent import runs, each concurrent import creates a concurrent import set record. All related import sets, concurrent import set jobs, and transform histories are shown in the form view.

Role required: import_admin

1. Navigate to **System Import Sets > Concurrent Import Set Jobs**.
2. Select the scheduled import for which you want to check status.
3. In the Related Links, reprocess or continue import sets, check the status of import sets or concurrent import set jobs, or view transform history.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reprocess</td>
<td>Start another scheduled import to reprocess the records.</td>
</tr>
<tr>
<td>Continue</td>
<td>Restart a scheduled import that was not completed.</td>
</tr>
<tr>
<td>Import Sets</td>
<td>State of import sets.</td>
</tr>
<tr>
<td></td>
<td><strong>State</strong></td>
</tr>
<tr>
<td></td>
<td>• Pending if the system has not started processing the import set.</td>
</tr>
<tr>
<td></td>
<td>• Running if the system is processing the import set.</td>
</tr>
<tr>
<td></td>
<td>• Processed if the system has completed processing the import set.</td>
</tr>
<tr>
<td></td>
<td>• Error if the import set processing failed.</td>
</tr>
</tbody>
</table>

Select an import set to see processing details for Import Set Runs and Import Set Rows for the import set.

<table>
<thead>
<tr>
<th>Concurrent Import Set Jobs</th>
<th>Type and state of concurrent import set jobs:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Type</strong></td>
</tr>
<tr>
<td></td>
<td>• Regular if you are running the scheduled import for the first time.</td>
</tr>
<tr>
<td></td>
<td>• Reprocessing if you are rerunning the scheduled import.</td>
</tr>
<tr>
<td></td>
<td>• Resuming if you are resuming a scheduled import that had an error.</td>
</tr>
<tr>
<td></td>
<td><strong>State</strong></td>
</tr>
<tr>
<td></td>
<td>• Pending if the system has not started processing the import set.</td>
</tr>
<tr>
<td></td>
<td>• Running if the system is processing the import set.</td>
</tr>
<tr>
<td></td>
<td>• Completed if the system has completed processing the import set.</td>
</tr>
<tr>
<td></td>
<td>• Error if the import set processing failed.</td>
</tr>
</tbody>
</table>

Select an import set job to see processing details for Import Set Runs and Import Set Rows for the import set job.

<table>
<thead>
<tr>
<th>Transform Histories</th>
<th>Check statistics in the transform histories for the scheduled import.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Select a start time to see Import Set Row Errors (including error codes and messages) and the Import Log for the scheduled import.</td>
</tr>
</tbody>
</table>

### Monitor concurrent import set jobs

Check the status of concurrent import set jobs.

Role required: import_admin

1. Navigate to **System Import Sets > Concurrent Import Set Jobs**.
2. Review the **Type** and **State** of each parent import set job.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>Type of concurrent import set job:</td>
</tr>
<tr>
<td></td>
<td>• Regular if you are running the scheduled import for the first time</td>
</tr>
<tr>
<td></td>
<td>• Reprocessing if you are rerunning the scheduled import</td>
</tr>
<tr>
<td></td>
<td>• Resuming if you are resuming a scheduled import that had an error</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>State</td>
<td>Status of the import set job:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Pending</strong> if import processing has not started</td>
</tr>
<tr>
<td></td>
<td>• <strong>Running</strong> when import processing has started</td>
</tr>
<tr>
<td></td>
<td>• <strong>Completed</strong> when import processing has finished</td>
</tr>
<tr>
<td></td>
<td>• <strong>Error</strong> if import processing did not finish successfully</td>
</tr>
</tbody>
</table>

3. Select a parent import set job to review the **Type** and **State** of each of its child import set jobs.

**Post CSV or Excel files directly to an import set**

An administrator can post CSV or Excel files directly to an instance.

Role required: import_set_loader

The `sys_import.do` target lets you dynamically upload a CSV or Excel file into the import set table specified by the `sysparm_import_set_tablename` parameter. You must specify a name that matches an existing import set table name. If the import set table does not exist, pre-create it by performing a manual import. The `sysparm_transform_after_load=true` parameter causes the CSV transform to be executed immediately, if a transform map exists.

You can upload a file using POST to the following URL (replace placeholders with desired values):

```
https://<instance>.service-now.com/sys_import.do?
sysparm_import_set_tablename=<table_name>&sysparm_transform_after_load=<true>
```

**Important:** The body of the POST must contain the file as a multi-part attachment.

**Posting a CSV file - Perl and Java examples**

An example using Perl to post a CSV file with basic auth credentials and Java Apache HttpClient class to post a CSV file with basic auth credentials.

**Perl example**

```perl
# file: uploadafile.pl
# call me like this:
# uploadafile.pl --url="https://instance.service-now.com/sys_import.do?
sysparm_import_set_tablename=dloo_test&sysparm_transform_after_load=true"
# --uploadfile=/Users/davidloo/Desktop/test_files/test_users.csv
#
# the "sysparm_transform_after_load=true" parameter instructs the import set
to transform immediately after loading
#
# use strict;
use LWP::UserAgent;
use HTTP::Request::Common;
use Getopt::Long;
use File::Basename;

my ( $o_url, $o_fqn );
GetOptions(
   "url=s"      => \$o_url,
   "uploadfile=s" => \$o_fqn,
);
#
```
```perl
$usage unless ( $o_url && $o_fqn );
my $url   = $o_url;
my $fname = $o_fqn;

# put timeouts, proxy etc into the useragent if needed
my $ua  = LWP::UserAgent->new();

# setup basic authentication credentials
$ua->credentials(
    'demo.service-now.com:443',
    'Service-now',
    'admin' => 'admin'
);

my $req = POST $url, Content_Type => 'form-data',
    Content => [
        submit => 1,
        upfile => [ $fname ]
    ];
my $response = $ua->request($req);

if ($response->is_success()) {
    print "OK: ", $response->content;
} else {
    print $response->as_string;
}
exit;

sub usage {
    printf "usage:&nbsp;%s --url=%s --uploadfile=%s\n",
        basename($0),'https://....','c:/data/test.csv';
    exit
}
```

**Java example**

**Attention:** The Apache HttpClient may limit the amount of data you can import in a single transaction. This example is meant as a starting point and should not be used in production.

```java
HttpClient httpclient = new HttpClient();
PostMethod post = new PostMethod("https://instance-name.service-now.com/
    sys_import.do?sysparm_import_set_tablename=u_test_upload&sysparm_transform_after_load=true");
try {
    Credentials defaultcreds = new UsernamePasswordCredentials("admin",
        "admin");
    httpclient.getState().setCredentials(AuthScope.ANY, defaultcreds); // Prepare HTTP post
    httpclient.getParams().setAuthenticationPreemptive(true);

    File targetFile = new File("/Users/davidloo/Desktop/test_files/
        nodeinfo2736820198834983863.csv");
    Part[] parts = { new FilePart(targetFile.getName(), targetFile) };
```
post.setRequestEntity(new MultipartRequestEntity(parts, post.getParams()));

    int result = httpClient.executeMethod(post);

    // Display status code
    System.out.println("Response status code: "+result);

    // Display response
    System.out.println("Response body: "+post.getResponseBodyAsString());
} catch(Exception e) {
    System.err.println(e.getMessage());
} finally {
    // Release current connection to the connection pool
    // once you are done
    post.releaseConnection();
}

Delete import sets

Delete import sets to clean up your database on a scheduled basis, one time only, or on demand.

Role required: admin

1. Navigate to **System Import Sets > Import Set Tables > Scheduled Cleanup.**
2. Fill out the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Defaults to <strong>Import Set Deleter.</strong> You can change the name if desired.</td>
</tr>
<tr>
<td>Active</td>
<td>Checked if the schedule is active. Unchecked if the schedule is not active.</td>
</tr>
<tr>
<td>Run</td>
<td>Specifies the frequency of the Import Set Deleter: Daily, Weekly, Monthly, Periodically, Once, or On Demand.</td>
</tr>
<tr>
<td>Time</td>
<td>Specifies up to three times of day to run the Import Set Deleter.</td>
</tr>
<tr>
<td>Application</td>
<td>Defaults to <strong>Global</strong> and can't be changed.</td>
</tr>
<tr>
<td>Conditional</td>
<td>Checked if the Import Set Deleter must meet specified conditions. Unchecked if the Import Set Deleter doesn't have to meet any conditions.</td>
</tr>
<tr>
<td>Run this script</td>
<td>The script that performs the deletion. Defaults to deleting import sets and their related import set rows that were created more than seven days ago.</td>
</tr>
<tr>
<td>Day</td>
<td>The day of the week for weekly runs, or the day of the month for monthly runs.</td>
</tr>
<tr>
<td>Repeat Interval</td>
<td>The number of days in the repeat interval and up to three times of day for the repeat interval.</td>
</tr>
<tr>
<td>Starting</td>
<td>The starting date and time for the periodical run or the one-time run.</td>
</tr>
</tbody>
</table>

3. Click **Update** to update the schedule, or click **Execute Now** to run the Import Set Deleter immediately.
Delete import set tables

Delete import set tables, related transform maps, or data only (preserving the table structure) to clean up your database.

Role required: admin

1. Navigate to System Import Sets > Import Set Tables > Cleanup.
2. Move the tables you want to delete from Available tables for deletion to Delete these tables. Deleting any table deletes all records and removes the table.
3. Select the Delete related transform maps check box to delete the selected import set tables and their related transform maps. All records and all associated transform maps are removed. Deselect the check box if you don’t want to delete the related transform maps.
4. Select the Delete data only (preserve table structure) check box to delete the data only from the selected import set tables and preserve the table structure. All records are removed, but the tables remain intact. Deselect the check box if you want to delete the selected import set tables as well as the data in those tables.
5. Click Cleanup.

Import sets properties

Multiple properties control import set behavior.

Import sets properties

**glide.import_set.preserve.leading.spaces**

Specifies whether the import process preserves leading spaces in Excel data cells. When false, the import process removes leading spaces from Excel data cells. When true, the import process preserves leading spaces.

![Note: The import process always removes trailing spaces from Excel data cells.](image)

- Type: true | false
- Default value: false
- Location: Add the property

**glide.import_set_row.dynamically_add_fields**

Specifies whether an import set can add new columns to the staging table (true) or not (false). Instances that contain large numbers of import sets can sometimes become unresponsive when an import adds a column because the instance must alter every row in the staging table. In some cases, the database alter table action causes an outage. Setting this property to false prevents an import set from adding columns to the staging table and produces a log message. As a workaround, administrators can manually add a column to the staging table by creating a new dictionary entry and then reimporting the import set.

- Type: true | false
- Default value: true
- Location: Add the property

**com.glide.loader.verify_target_field_size**

Enables dynamic resizing of import set fields. By default, up to 20 records of the source data are sampled to determine the import set field length. If the field is empty in all the sampled records, the default length of 40 is used. Any data loaded that exceeds the import set table field length is truncated.

- Type: true | false
**glide.ds.file.http.variable_replacement**

Enables system property expansion for File-type data sources that are retrieved using HTTP or HTTPS.

- **Type:** true | false
- **Default value:** true
- **Location:** Add the property
- **More information:** Data source fields

**glide.scheduled_import.stop_on_error**

Set to true to stop the import process when the parent scheduled import generates an error. This behavior can be useful when one import set depends on the results of another import set.

- **Type:** true | false
- **Default value:** false
- **Location:** Add the property

**glide.impex.transformer.empty_value_nil**

Controls how empty string values are handled during transformation from an import set staging table. Set this property to true to preserve empty strings. Set this property to false to convert empty strings to the string NULL.

**Note:** An empty string is always stored as a null value in the database, regardless of this property value.

You can use this property when you run an onBefore script during transformation. Setting this property to true allows you to check for null values using hasValue() or nil() functions.

- **Type:** true | false
- **Default value:** false
- **Location:** Add the property

**com.glide.loader.max_scan_rows**

Controls how many rows of source data are sampled to automatically generate staging table fields when you import data. This property applies to JDBC, XLS, CSV, and XML imports but not to JSON and XSLX imports.

- **Type:** integer
- **Default value:** 20
- **Location:** Add the property

### Concurrent import sets properties

**glide.scheduled_import.max.concurrent.import_sets**

Maximum number of import sets for one concurrent import.

- **Type:** Integer
- **Default value:** 10
- **Location:** Add the property

**com.glide.concurrent_import_set_insert_mutex_spin_wait**
Wait time mutex spends if the lock is acquired (in milliseconds).

- Type: Integer
- Default value: 1000
- Location: Add the property

**com.glide.concurrent_import_set_insert_mutex_expiration**

Mutex expiration time (in milliseconds).

- Type: Integer
- Default value: 300000
- Location: Add the property

**com.glide.concurrent_import_set_mutex_fast_lock**

Specifies whether to use fast lock (true) or SQL-based slow lock (false).

- Type: true | false
- Default value: false
- Location: Add the property

### Web service import sets properties

**com.glide.ws_import_set.column_resize**

When true, enables dynamic column resizing on import staging tables for web service import sets.

- Type: true | false
- Default value: false
- Location: Add the property

**com.glide.ws_import_set.column_resize.max_row_count**

The maximum number of rows an import staging table can have for dynamic column resizing with web service import sets.

Import staging tables with more than this number of rows will not use dynamic resizing with web service import sets, even if **com.glide.ws_import_set.column_resize** is true.

This property has a maximum value of 500,000.

- Type: Integer
- Default value: 100,000
- Location: Add the property

### CSV properties

**com.glide.csv.loader.ignore_non_parseable_lines**

Allows an instance to ignore one or more lines (rows) that contain bad data in a CSV import, such as a row that is missing a column of data. By default, imports cannot ignore bad data in CSV files and fail on the first error.

- Type: true | false
- Default value: false
• Location: Add the property

**com.glide.csv.loader.max_errors_allowed**

Specifies the maximum number of lines (rows) that an import can ignore before failing. If the import succeeds, the import lists the number of rows the import ignored due to errors.

- Type: integer
- Default value: 100
- Location: Add the property

**glide.import.csv.charset**

The charset of the CSV file to import. Valid values are UTF-8 and WINDOWS-1252. You may need to use UTF-8 formatting when importing special characters.

- Type: String
- Default value: WINDOWS-1252
- Location: Add the property

**Excel import properties**

**glide.excel.multiplier**

The maximum amount of instance memory to allocate to an Excel import. This property applies when importing .XLS files only.

The value of this property is multiplied by the file size of the Excel file to determine the total memory allocation. The memory used cannot exceed the limit specified by the `glide.excel.max_memory_percent` property.

For example, with the default value 8 and a 10MB Excel file, the instance will use up to 80MB of memory for the import.

- Type: integer
- Default value: 8
- Location: Add the property

**glide.xlsx.multiplier**

The maximum amount of instance memory to allocate to an Excel import. This property applies when importing .XLSX files only.

The value of this property is multiplied by the file size of the Excel file to determine the total memory allocation. The memory used cannot exceed the limit specified by the `glide.excel.max_memory_percent` property.

For example, with the default value 10 and a 10MB Excel file, the instance will use up to 100MB of memory for the import.

**Note:** Do not modify the value of this property. The default value was selected for optimal performance.

- Type: integer
- Default value: 10
- Location: Add the property

**glide.excel.max_memory_percent**

The maximum amount of memory allowed for Excel imports, as a percentage of the total instance memory.
• Type: integer
• Default value: 20
• Location: Add the property

**glide.excel.use_disk_backed_strings_table**

Controls whether the instance uses disk storage to maintain large file data during XLSX import. Set this property to false to store XLSX file data only in memory. Setting this property to false increases the memory used during XLSX import.

• Type: true | false
• Default value: true
• Location: Add the property

**glide.excel.in_memory_strings_table_size_mb**

The maximum amount of memory, in megabytes, available to store XLSX file data before writing to disk storage when glide.excel.use_disk_backed_strings_table is true. Setting a lower value for this property will use less memory during XLSX import but may result in slower imports.

• Type: integer
• Default value: 5
• Location: Add the property

**glide.xlsx.import.debug**

Enables debug logging for XLSX imports.

• Type: true | false
• Default value: false
• Location: Add the property

**glide.import.excel.enhanced_number_conversions**

When true, numeric values greater than 10 million are preserved in import staging tables. When false, imported values greater than 10 million are converted to scientific notation that may not match the original imported value. This property should be set to true for importing most kinds of data.

• Type: true | false
• Default value: true
• Location: Add the property

**JDBC connection properties**

**glide.jdbcprobeloader.retry**

The number of times a JDBC probe loader attempts to process data returning from a JDBC data source. Sleeps on the value defined in glide.jdbcprobeloader.retry_millis between retries.

• Type: integer
• Default value: 60
• Location: Add the property

**glide.jdbcprobeloader.retry_millis**
How many milliseconds a JDBC probe loader waits in between retry attempts to process data from a JDBC data source.

- Type: integer
- Default value: 5000
- Location: Add the property

**Logging and debug properties**

**com.glide.import_set.importlog_level**

Specifies how much information import sets add to the log. Possible values are INFO, WARNING, and ERROR. You can set this to INFO in the dev environment and change it to WARNING or ERROR in production to reduce amount of logging noise traffic to the database.

**Note:** This property does not impact logging related to the cleanup of staging tables.

- Type: string
- Default value: INFO
- Location: Add the property

**glide.import.debug**

Enables debug logging for all import processes.

- Type: true | false
- Default value: false
- Location: Add the property

**glide.import.sftp.debug**

Enables additional debug logging for SFTP imports. Enabling this property will cause the instance to log all outgoing and incoming messages during the SSH session.

- Type: true | false
- Default value: false
- Location: Add the property

**glide.import.scp.debug**

Enables additional debug logging for SCP imports. Enabling this property will cause the instance to log all outgoing and incoming messages during the SSH session.

- Type: true | false
- Default value: false
- Location: Add the property
Web service import sets

Web service import sets complement direct web services and scripted SOAP web services providing a web service interface to import set tables.

Web service import set

By default, this type of web service transforms the incoming data synchronously based on the associated transform maps. If the associated import set mode is set to **Asynchronous**, the behavior is to save the data for transformation at a later time. Web service import sets tables publish all the default web service functions in the WSDL.

System web services

This plugin also provides the following standard import set tables:

- Computer
- Location
- Notification
- User

You can access a web service import set WSDL by specifying the import set table name + ".do?WSDL" on the URL. For example:

http://<instance name>.service-now.com/imp_notification.do?WSDL.
Creating an import set web service

Create a web service import set table to define how to stage and transform imported data.

Navigate to System Web Services > Create New.

![Create Web Service form]

Create Mapped Web Service

The Name of the web service is the table name of the import set table whereas the Label field is the resulting table field.

If you want to create a transform map after creating the web service, check the Create transform map checkbox and choose the target table you want the data to transform into. After the Create button is clicked, the web service will be created and you will be immediately put into the Table Transform Map form. You may then continue to specify the transform map or script.

Web Service Fields

The fields available for this web service. All fields by default are published as the XSD type of xsd:string. The Name is the field that is exposed for the web service and therefore appears as the name of the field in the WSDL. The Label is the label of the field as it appears for the import sets table.

You can Add, mark for Delete or modify (double-click the field) an existing web service field in this list.

Note: After adding web service fields, click Create to create the web service import set table.
To add other fields after the Web Service is created, find the target table, and add the fields to that table.

**Mapping web service import sets**

During the creation of the web service import set, you may optionally create the transform map for it. All transform maps are executed for the service when it is invoked and the import set mode is set as "Synchronous" (the default).

The following image is an example of the transform map associated with the Notification web service import set.
Soap Transform Map

Related Links

Mapping Assist
Auto map matching fields
Adding Web Service Response Values

In the transform map script associated with a web service import set, some variable values can change the response values of the web service. In addition to the normal variables that are available in a transform map script, the table documents the variables that are available and their effects.

**Adding Web Service Response Values**

<table>
<thead>
<tr>
<th>Variable name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>response</td>
<td>Output Object</td>
<td>Javascript object that holds dynamically created response elements used to customize the output response of a web service import set insert.</td>
</tr>
</tbody>
</table>

**Example**

```
// create new elements called "transaction_id"
// and "hello" in the web service response
response.transaction_id="abc123";
response.hello="world";

status_message="message 1";
// this is the normal status_message variable
```

The code snippet example results in the following response being generated back to the web service consumer

```xml
<soapenv:Envelope
 xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
 xmlns:imp="http://www.service-now.com/imp_notification"
><soapenv:Header/>
<soapenv:Body><soapenv:Header/>
<soapenv:Body><soapenv:Body>
<insertResponse
 xmlns="http://www.service-now.com/imp_notification"
><sys_id>969d157c0a0a0baf008ba5770ffa798c</sys_id>
<table>incident</table>
<display_name>number</display_name>
<display_value>INC0010091</display_value>
<status>inserted</status>
<status_message>message 1</status_message>
<transaction_id>abc123</transaction_id>
<hello>world</hello>
</insertResponse>
</soapenv:Body></soapenv:Envelope>
```

**Debugging web service import sets**

To debug a SOAP Request coming into the system, create the system property `glide.processor.debug.SOAPProcessor`. Once you have created it, set it to `true` to have all SOAP requests be logged in the System Log. Set it to `false` when you are done to keep the size of your System Log to a managed length.
Web service import set mode

When a SOAP message inserts a record into an import set table, and there is no import set for that table in the **Loading** state, a new import set will be created with the **Mode** set to **Synchronous**.

An import set with a **Mode** of **Synchronous** will transform the data as soon as it is inserted (provided that the transform map already exists). This import set will also have a default **State** of **Loading**. By default, all **Synchronous** import sets will automatically be modified to **Processed** at midnight. As a result, when a new insert happens to the same table, a new **Synchronous** import set will be created.

<table>
<thead>
<tr>
<th>Number</th>
<th>Created</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISET10009</td>
<td>2009-01-12 15:50:27</td>
</tr>
</tbody>
</table>

**Synchronous** import set

Changing this import set to a **mode** of **Asynchronous** and a **state** of **Loading** has the effect of not transforming the incoming data as it is inserted, but rather "loading" the import set and deferring the data transformation later, either manually, or with a scheduled script job.

<table>
<thead>
<tr>
<th>Mode</th>
<th>State</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asynchronous</td>
<td>Loading</td>
<td>Data transformation is not occurring automatically and immediately. Data added to import set row has a state of &quot;Pending&quot;. Transform can be scheduled or executed manually when state is changed to <strong>Loaded</strong>.</td>
</tr>
<tr>
<td>Asynchronous</td>
<td>Loaded</td>
<td>Marks the completion of data loading. Data transformation can now occur in a scheduled fashion or manually.</td>
</tr>
<tr>
<td>Synchronous</td>
<td>Loading</td>
<td>Data transformation is occurring automatically and immediately whenever data is inserted into the associated import set row.</td>
</tr>
</tbody>
</table>
Controlling Insert Behavior

In imports sets that specify one or more coalesce fields, records with a matching coalesce value are transformed from source to target table serially (one at a time) to prevent duplicates. In import sets that do not specify any coalesce field, records are transformed concurrently. You can control this behavior using the `glide.import_set_insert_serialized_when_no_coalesce` property.

The `glide.import_set_insert_serialized.<table name>` system property controls how the instance inserts records from web service calls into a specific import set table. When true, this property prevents identical simultaneous inserts from creating duplicate records by serializing the database insert operations. If a target table does not have any coalesce fields defined in a transform map, set this property to `false` to improve web service import set performance.

**Note:** Setting this property to `false` can result in the creation of duplicate records.

**Note:** The `glide.soap.import_set_insert_serialized.<table name>` system property provides equivalent functionality to `glide.import_set_insert_serialized.<table name>`, but if both properties are defined, `glide.import_set_insert_serialized.<table name>` supersedes `glide.soap.import_set_insert_serialized.<table name>`.

Standard SOAP Response

The SOAP response from a web service import set `insert` call returns the following standard values:

```xml
 xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
  <SOAP-ENV:Body><insertResponse><sys_id>fa648f5f0a0a0b2b0048e7012448b8f1</sys_id><table>incident</table><display_name>number</display_name><display_value>INC10014</display_value><status>inserted</status></insertResponse></SOAP-ENV:Body></SOAP-ENV:Envelope>
```
### Standard SOAP Response

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sys_id</td>
<td>The Sys_id of the resulting record that was created or modified</td>
</tr>
<tr>
<td>table</td>
<td>The table name of the table that was affected. In the case of an <strong>Asynchronous</strong> call, the table name would be the import set table eg. imp_notification for the <strong>Notifications</strong> web service import set table</td>
</tr>
<tr>
<td>display_name</td>
<td>The name of the field that is set as the display field for the record that was created or modified</td>
</tr>
<tr>
<td>display_value</td>
<td>The value of the field designated as the display field. For example, the display field for the <strong>Incident</strong> table is the <strong>Number</strong> field and an example value would be INC10001</td>
</tr>
<tr>
<td>status</td>
<td>A string value that indicates the action that occurred as a result of the web service invocation, relating to the record defined by the sys_id and table field values</td>
</tr>
<tr>
<td></td>
<td>• <strong>inserted</strong> - the record was inserted</td>
</tr>
<tr>
<td></td>
<td>• <strong>updated</strong> - the record was updated</td>
</tr>
<tr>
<td></td>
<td>• <strong>ignored</strong> - the input was ignored, the record was not updated and no new record was created</td>
</tr>
<tr>
<td></td>
<td>• <strong>skipped</strong> - the input data was skipped (similar to ignored) due to missing coalesce values</td>
</tr>
<tr>
<td></td>
<td>• <strong>error</strong> - there was an error processing the input</td>
</tr>
<tr>
<td>status_message</td>
<td>This value translates to the value found in the Comment field of the import set row and usually contains information related to the status value eg. &quot;No field values changed&quot; when the status is &quot;ignored&quot;. Setting this value to a customized string value will cause the SOAP response to contain an optional status_message field to be returned</td>
</tr>
<tr>
<td>error_message</td>
<td>The message related to a status of <strong>error</strong>. When an error occurs, setting this value to a customized string value will cause the SOAP response to contain an optional error_message field to be returned</td>
</tr>
</tbody>
</table>

### Tailoring the SOAP Response

It is possible to include information other than the information specified in the WSDL by overwriting the contents of **status_message** using the transform script.

### Inserting multiple records using insertMultiple

You can insert multiple records in one SOAP request by using the insertMultiple operation.

By default, insertMultiple operations create new import sets in **Synchronous** mode. To process new import sets asynchronously, activate the business rule Insert multiple asynchronous mode.

The insertMultiple operation is available for the Direct Web Service API and Web Service Import Sets. To enable insertMultiple, activate the Insert Multiple Web Service plugin.
**Web service import sets security requirements**

Web Service Import Sets use the same security mechanisms as SOAP Web Services.

- Basic authentication requires a Web Service user provide a valid user name and password.
- Contextual security requires a Web Service user meet the access control rule of the queried table.

If your instance uses high security settings, the Web Service user may also need the `soap` role.

**Web service import sets related links**

When displaying a mapped web service table, you have the following related links.

- Import Sets — The import sets related to this web service import set.
- Transform Maps — A list of transform maps related to this web service.
- Transform History — The transformation history.
- Edit Web Service — Edit the web service.

The following image shows a record that was inserted into the web service import set Notification. The target record is the resulting creation or modification to the Incident table record as a result of the transform.
Web service import sets example

This example demonstrates the WSDL, SOAP envelope and response, Perl invocation, and result of a SOAP web service import.

Sample WSDL

```xml
<?xml version="1.0" encoding="UTF-8"?>
```
Sample SOAP Envelope

```xml
```

Sample SOAP Response

```xml
  <SOAP-ENV:Body>
    <insertResponse>
      <sys_id>b54aafbf0a8006f0058db95daa5b88d</sys_id>
      <table>incident</table>
      <display_name>number</display_name>
      <display_value>INC10008</display_value>
      <status>ignored</status>
      <status_message>No field values changed</status_message>
    </insertResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Example Invocation using Perl

The following example script uses the Notification web service to create an Incident as the itil user. It uses the Perl language and the SOAP::Lite package.

```perl
#!/usr/bin/perl -w
use SOAP::Lite ( +trace => all, maptype => {} );use SOAP::Lite;
sub SOAP::Transport::HTTP::Client::get_basic_credentials{return 'itil': 'itil';} // set basic auth credentials for the itil user
my $soap = SOAP::Lite->proxy('http://localhost:8080/glide/imp_notification.do? SOAP');
my $method = SOAP::Data->name('insert')->;attr({xmlns => 'http://www.service-now.com/'}); # insert into the web servicemy@params=( SOAP::Data->name(message =>'problem detected for database DB12DG'));push(@params, SOAP::Data->name(source =>'DB12DG'));push(@params, SOAP::Data->name(uuid =>'HGAF76251HGF2'));
my $result = $soap->call($method => @params);
print_fault($result); // print any SOAP faults
print_result($result); // print any results
sub print_result {my ($result) = @_; if ($result->body && $result->body->{insertResponse}) {
my $keyHash = %{$result->body->
```
The following is the result printed by the Perl script on the console:

```
name=display_value   value=INC10011
name=status   value=inserted
name=table   value=incident
name=display_name   value=number
name=sys_id   value=cd45649c0a0a0b2b00e6f27649d6b2c
```

The following image shows the resultant row created for the import set table **Notification** (imp_notification).

**Easy import**

Easy import is a simplified import process that enables you to import only the columns you want.

Only admins can use easy import. You can import data to tables within the current scope and tables that grant write access to other applications.

**Easy import template validation**

Each import template must pass two sets of validation:

<table>
<thead>
<tr>
<th>Type of validation</th>
<th>Stored in</th>
<th>Results of failing validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client-side validation</td>
<td>Import template</td>
<td>The template highlights the invalid cell.</td>
</tr>
</tbody>
</table>
### Download an import template

Select the list you want to import data to and create an import template from that list.

Role required: admin

1. Navigate to any list, such as **Self-Service > Incidents**.
2. Right-click the column heading.
3. Select **Import**.
4. Select if you want to **Insert** or **Update** records.

<table>
<thead>
<tr>
<th>Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insert</td>
<td>Use this template to add new records to a table.</td>
</tr>
<tr>
<td>Update</td>
<td>Use this template to change values within existing records in a table. This template contains one row for each record in the list. The current list filter determines what records the template contains.</td>
</tr>
</tbody>
</table>

5. Optional: Clear the **Include all fields in the template?** check box to include only columns that appear in the list in the template. Certain fields in the table are updated by system processes, and you cannot import values into them. An example is the **Created by** field, which is populated during import with the logged-in user who performs the import.

   Leave this check box selected to include all columns from the table in the template, even those columns that are hidden in the list.

6. Select the **Export template format** you want, either **XLS** or **XLSX**.

   XLSX is the preferred format, XLS is available for legacy support. The **Export template format** field appears only if the property `glide.legacy.excel.export` is true.
7. Click **Create Excel template**.

Open the spreadsheet using your preferred application.

**Note:** Each template contains a **Directions** tab describing how to use the template.

**Add a record in the template**

Add rows to the template to create new records.

Role required: admin

**Note:** The template only imports records on the first page of the template. The import process ignores all other pages.

**Easy import insert template**

1. Add a row for each record you want to add to the table. Each column corresponds to a field in the target table. Use the UI field hints to learn about the purpose and content of the field.

   The template validates values as you enter them and highlights cells containing invalid data. While you do not have to provide a value for every column, certain fields may fail validation if you do not provide a value.

2. Review any highlighted cell and resolve the issue.

3. When you finish entering new rows, save the spreadsheet as an Excel Workbook.

   The insert templates use special processing for certain fields:
   - **Created by Field**: The insert template always lists the system administrator user (admin role) in the Created by field regardless of whether the import includes a Created by column. Even if you provide a different user value in the template, the import process overwrites this value with the system administrator user.
   - **Blank Values**: Leaving a cell blank in the insert template results in a blank value in the imported record, provided the field supports a blank value. Fields that do not support a blank value will produce a validation error if you provide a blank value.
Update a record in the template

Modify rows in the template to update existing records.

Role required: admin

Note: The template only imports records on the first page of the template. The import process ignores all other pages.

Easy import update template

1. Edit the row for each existing record to be updated. Replace existing values with new values. Use the UI field hints to learn about the purpose and content of the field.

   The template validates values as you enter them and highlights cells containing invalid data. While you do not have to provide a value for every column, certain fields may fail validation if you do not provide a value.

2. Review any highlighted cell and resolve the issue.

3. When you finish updating existing rows, save the spreadsheet as an Excel Workbook (.xls).

The insert templates uses special processing for certain fields:

- **Updated by Field**: The update template always lists the system administrator user (admin role) in the Updated by field regardless of whether the import includes an Updated by column. Even if you provide a different user value in the template, the import process overwrites this value with the system administrator user.

- **Blank Values**: The update template uses these rules when handling blank values in spreadsheet cells.

### Blank values

<table>
<thead>
<tr>
<th>Original Value</th>
<th>New Value</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blank value</td>
<td>Any non-blank value</td>
<td>Valid update: the update changes the blank value to the new value.</td>
</tr>
<tr>
<td>Any non-blank value</td>
<td>Blank value</td>
<td>Invalid update: the update preserves the existing non-blank value.</td>
</tr>
</tbody>
</table>
**Import a record from the template**

After updating the import template with new data, import the template to your instance.

Role required: admin

1. Navigate to the same list you used to download the import template.
2. Perform the appropriate action for the list version.

<table>
<thead>
<tr>
<th>Action</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>List v2</td>
<td>Right-click the column heading and select <strong>Import</strong></td>
</tr>
<tr>
<td>Action</td>
<td>Version</td>
</tr>
<tr>
<td>--------</td>
<td>---------</td>
</tr>
<tr>
<td>List v3</td>
<td>Open the list title menu and select <strong>Import</strong>.</td>
</tr>
</tbody>
</table>

To import external data into Incident:

1. Insert or update existing records using an Excel template file. Click **Upload** to preview the data to be imported. 

   ![Image of import options]

   **Do you want to insert or update data?**
   - [ ] Insert
   - [ ] Update

   **Do you want to create an Excel template to enter data?**
   - [x] Yes

   **Step 1: Create an Excel template file to enter data**
   - Include all fields in the template? [x]
   - [Create Excel template]

   **Step 2: Upload the template file**
   - Excel template file: [Choose File] No file chosen
   - [Upload]

2. From **Insert or update**, select the import type.
3. From **File**, select the import template to import.
5. Click **Upload and Preview Import Data**.

ServiceNow validates the template.

If the template passes validation and the imported preview matches your expectations, click **Complete Import** to import records into the current table. If the template fails validation, review the errors. Click **Ignore Errors and Complete Import** to continue the import by skipping any bad data cells.

---

**Show reference fields as lists in Excel templates**

Display selected reference fields as lists in Excel templates to simplify data selection and updates.

When you do an Easy Import and export the data to an Excel spreadsheet, you may want to convert some cells to lists. For example, in the Incident [sys_incident] record, you may want the **Assigned to** field options to appear as a list to enable you to select or update the person assigned to the incident.

Role required: admin

1. Navigate to the record for which you want to create lists.
2. Go to the field you want to appear as a list. Right-click the field name and select **Configure Dictionary**.
3. In the **Attributes** field of the Dictionary Entry page, enter the following attribute: `easy_import_ref_as_choice=true`. Save your dictionary entry.

You can also enter other **Attributes** for the dictionary entry. For example, there is a default limit of 250 entries in a list. If there are more than 250 entry options for a field, the entries do not appear in list format, but as a single entry. Assume that there are 500+ entry options. You can enter the following attribute in the dictionary entry for a field to set a higher limit of 600 entry options for that field: `easy_import_ref_query_limit=600`. The Excel spreadsheet now displays the field as a list of up to 600 options.

You can set a system-wide limit for the number of entry options at a field by entering a value for the `glide.easy_import.reference_query_limit` system property. If the system property is not present or not set and the `easy_import_ref_query_limit` attribute is not set for the field, the default limit of 250 entry options applies. The attribute always takes priority over the property: If both the attribute and the property are set, the attribute value is used.
4. Repeat steps 2-3 for any other fields you want to appear as lists in the Excel output. The field appears as a list on the Excel spreadsheet:

![Excel spreadsheet with list of names]

### Easy import template validation

Each import template must pass two sets of validation.

<table>
<thead>
<tr>
<th>Template validation</th>
<th>Stored in</th>
<th>Results of failing validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client-side validation</td>
<td>Import template</td>
<td>The template highlights the invalid cell.</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Type of validation</th>
<th>Stored in</th>
<th>Results of failing validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server-side validation</td>
<td>Instance</td>
<td>The import pauses and displays an error message.</td>
</tr>
</tbody>
</table>

**Template data validation**
Some cells in the template contain calculations or validation rules. These rules are intended to help you enter data that is appropriate for the field (column).

If you want to paste data from another spreadsheet, use the **Paste Special** command to paste only values or match the existing formatting.

![Easy import paste special](image)
Paste special values only

Template type validations
Server-side validation verifies that the import template contains the necessary format.

Template type validation

<table>
<thead>
<tr>
<th>Template type</th>
<th>Validation done</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insert template</td>
<td>• Template contains a header row with valid field names.</td>
</tr>
<tr>
<td></td>
<td>• Template contains one or more data rows.</td>
</tr>
<tr>
<td></td>
<td>• Template does not contain a sys_id column.</td>
</tr>
<tr>
<td>Update template</td>
<td>• Template contains a header row with valid field names.</td>
</tr>
<tr>
<td></td>
<td>• Template contains one or more data rows.</td>
</tr>
<tr>
<td></td>
<td>• Template contains a sys_id column to match a row to an existing record.</td>
</tr>
</tbody>
</table>
Data type validations
Both client-side and server-side validation verify that template cells contain data that matches the ServiceNow field type.

Data type validations

<table>
<thead>
<tr>
<th>ServiceNow field type</th>
<th>Validation done</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choice list</td>
<td>Cell contains a value that matches a choice option from the choice list.</td>
</tr>
<tr>
<td>Integer</td>
<td>Cell contains a number without any decimal points.</td>
</tr>
<tr>
<td>Reference</td>
<td>Cell contains a value that matches an existing related record. This validation applies only to fields in which the list of possible choices is relatively small and mostly static. It does not apply to fields such as ‘Assigned To’ in which the list of possible choices is dynamic and large. Validation takes place when the data is inserted into the database, but not in Excel.</td>
</tr>
<tr>
<td>True</td>
<td>False</td>
</tr>
</tbody>
</table>

Note: When you enter reference field values in the Excel spreadsheet, enter the display value and not the sys_id of the referenced record. Enter this value the same as you would on a form. For example, for a reference to a user record, enter the username.

Easy import properties
Several properties control the behavior of easy import.

glide.import_template.row_limit
Controls the maximum number of rows included in an easy import template. By default, if a table contains more than 10,000 records, only the first 10,000 are exported.

- Type: Integer
- Default value: 10,000
- Location: Add the property

glide.easy_import.run_business_rules
When true, business rules, workflows, approval engines, auditing, and field normalization apply when easy import inserts or updates data. This functionality is equivalent to setting GlideRecord.setWorkflow() to true or false.

- Type: true | false
- Default value: true
- Location: Add the property

glide.import_template.field_types_to_ignore
A list of fields that will be ignored when a record is imported with easy import feature.

- Type: String
Troubleshoot import set performance

Review these performance issues to troubleshoot and improve the performance of your import set jobs.

Running business rules during transform

Running business rules during transform may cause the transform to take longer than expected, or cause the instance to slow down.

**Becomes an issue:** When importing a very large amount of data. For example, importing all data from an old system.

**Symptoms:** The transform takes much longer than expected. Also, the entire instance may be slow during that time.

**How to avoid this:** Do not run items like business rules, workflows, approval engines, and so on during a transform unless you want all insert and update business rules, notifications, and workflows to run. For example, when importing all data from an old system, you may not want notifications to run. To disable these items from running and to cease auditing and field normalization within the transform map for that import, deselect the Run business rules check box.

![Transform Map Checkbox](image)

**Note:** Consider using an onComplete transform script to run business logic such as calculations at the end of an import rather than on each record as business rules do.

Slow transform scripts

Using multiple GlideRecord queries or large loops may slow down transform scripts.

**Becomes an issue:** When the transform scripts are using multiple GlideRecord queries or looping through large collections of objects for each row. This issue may appear when the transform script is not efficient. In most cases, script goals can be accomplished using built-in functionality within the Import Set application. For example, you can script case-sensitive coalesce instead of writing scripts that use GlideRecord queries. GlideRecord queries typically slow down the import.
**Symptoms:** The transform takes much longer than would be expected. Depending on the script, the entire instance may be slow during that time.

**How to avoid this:** Use base system functionality whenever possible instead of writing custom scripts and if you do write scripts, avoid writing complicated scripts that use GlideRecord queries.

**Importing data that has not changed**
Repeatedly importing data that has not changed leads to many skipped rows.

**Becomes an issue:** When a customer is importing data from a table that is very large and most of the records are not getting updated on a regular basis.

**Symptoms:** The import set takes longer than expected. Under **System Import Sets > Progress**, expect to see an import with a **Total count** that is very high with a **Skipped count** that is also very high - this is found under the **Message** column. Indicating that most of the records imported had not actually changed. These records did not need to be imported.

**How to avoid this:** If you are running a JDBC import, use the last run datetime option in your import set **Data Source**. For a type of File import, be sure that whatever is generating your files is only adding data that is new, or has been changed.

**Coalescing on non-indexed fields**
Coalescing on non-indexed fields with a large amount of data may cause transforms to slow down.

**Becomes an issue:** When matching on fields that are not indexed, this causes the transform stage of an import to run slowly. However, it only becomes an issue if there is a large enough amount of data. In extreme cases, this causes performance issues with the database due to added load.

**Symptoms:** Time spent in the transform stage of the import is large relative to the time taken to load the data. Expect to see high transform times.

**How to avoid this:** If possible, you should coalesce on a field that unique and already indexed. To determine if a field is already indexed, navigate to **System Definition > Tables & Columns** and find the table. In the list of columns for that table, an indexed column has a blue icon with an i next to it if indexed. For assistance indexing a field contact ServiceNow Technical Support.

**Running imports simultaneously**
Running imports simultaneously may cause excessive load on the database.

**Becomes an issue:** When importing large amounts of data puts an additional load on the database. For example, importing 500,000 users and importing 200,000 configuration items at the same time. This can have a significant performance impact on all queries on the system due to the increased load on the database. This issue is especially severe when two imports are importing to the same table. In such a case, there is a possible contention issue for the table. Additionally, depending on which table is involved in processing, this can severely degrade performance of the import and the instance.

**Symptoms:** Multiple simultaneous imports running slowly combined with load on the database. You see large numbers of inserts and updates along; and if there is enough load or contention, high IO Wait times.

**How to avoid this:** Stagger your imports so they do not overlap.

**Large import set tables**
Failing to clean import set tables may lead to those tables becoming cluttered and slow.

**Becomes an issue:** When the **Import Set Deleter** job is not running.

**Symptoms:** This is a size issue. If the import sets are not cleaned on a regular basis (a cleanup is recommended after seven days worth of data) the table fills causing imports to stop.
**How to avoid this:** Verify the *Import Set Deleter* job is running. If it is not currently running, contact Customer Service and Support as they will truncate all import set tables before enabling this job.

**Altering table schema during import**

Changing the table schema, such as by importing a new column locks the import set table.

**Becomes an issue:** Any time a new column is imported, the entire import set table is locked during that schema change and depending on the size of the table, can take between five and ten minutes. During that time, no data can be selected or inserted. If that table is not used often, this may not cause any problems. However, if that table is frequently used, for example the LDAP import table, issues may arise.

**Symptoms:** The symptoms of this problem may vary. In our example of the LDAP import table, any transactions requiring a query of the LDAP import table will have to wait until the schema change has completed. As the LDAP import table is used when logging into the instance, no users are able to log in while the schema change is happening.

**How to avoid this:** Truncate the import table before importing with a new column.

**Importing very large data sets**

Importing a very large data set takes longer than importing multiple smaller data sets.

**Becomes an issue:** When very large data sets are imported in a single job.

**Symptoms:** The import job takes a long time to complete.

**How to avoid this:** Break a very large data set into multiple, smaller jobs for faster results. Consider import sets under 100,000 records as a guideline. For example, importing 10 sets of 100,000 records completes faster than one import of 1 million records even though the total data imported is the same.

**Importing from another ServiceNow instance**

There are several methods for moving data from one instance to another.

All of these methods assume you need to periodically move a collection of records from a table on one instance to a table on another instance. If you want an action on an individual record to trigger a corresponding action on another instance, consider using a REST web service instead.

**Identifying Needed Related Records**

All import processes work by fetching data from one table at a time. This process can produce unexpected results if the incoming data references new records in other tables such as users, locations, or companies. To prevent importing broken references to other tables you must identify the connections between your tables and import the common data prior to importing the application data.

For example, prior to importing incident data, you might want to first import related configuration items, users, and locations. Furthermore you might want to import incidents before importing problems or changes that refer to these incident records.

**Available Import Processes**

The system offers the following processes to move data from one instance to another.

- Export and import XML records directly from lists
- Create XML import sets and transform data as needed
- Export and import CSV files from lists
XML records from lists

You can directly export records as XML from any list or form.

This export process preserves all record field values including system generated field values such as:

- Sys ID
- Creation date
- Update date

The XML import process directly inserts records into the target table. During the import the system:

- Ignores any business rules that normally apply to the table.
- Does not provide any opportunity to transform incoming data.
- Automatically matches a reference field's display value to the local Sys ID for some tables.

This process is good for directly copying records from one system to another but does not remove the need to know the relationships between tables. If you need validate or transform data or reconcile the sys ID values of reference fields, use an XML import set instead.

Automatic matching of display values

During the import of XML records, the system attempts to match some reference field display values to a local sys_id value.

If the system finds an existing record with a matching display value on the local instance, the import uses the sys_id of the existing record rather than the sys_id of the imported record.

For example, suppose you export an incident record that is assigned to the user John Smith. In the exported XML file there is an entry such as:

```
<incident>
  ...
  <assigned_to display_value="John Smith">7712173d2ba80200c5244f74b4da159a</assigned_to>
  ...
</incident>
```

This user already exists on the target instance but has a different sys_id value such as:

```
<sys_user><name>John Smith</name>
  ...
  <sys_id>18cab8de2be80200c5244f74b4da15f7</sys_id>
  ...
</sys_user>
```

Since the display value matches an existing record, the system uses the local instance's existing sys_id value for the reference field such as:

```
<incident>
  ...
  <assigned_to display_value="John Smith">18cab8de2be80200c5244f74b4da15f7</assigned_to>
  ...
</incident>
```

The system can match display values for the following tables.

- User [sys_user]
- Group [sys_user_group]
- Role [sys_user_role]
Using XML import sets

Use an XML import set to import data from another instance.

This method allows you to:

- Apply business rules
- Transform incoming data
- Reconcile sys_id values if necessary

Note: Administrators cannot set the update_synch attribute in Dictionary records to move data as part of update sets. This attribute was being used incorrectly to migrate data in large tables and was causing significant performance problems.

Create an XML data source to another instance

Data sources are used to create an import set so that data can be processed, if necessary, prior to being mapped onto a production table.

Note: To import using XML with High Security Settings enabled, you must possess elevated privileges.

1. Navigate to System Import Sets > Administration > Data Sources.
2. Click New.
3. Complete the form using the following values:

<table>
<thead>
<tr>
<th>Format</th>
<th>XML</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import set table label</td>
<td>&lt;import_set_table_label&gt;</td>
</tr>
<tr>
<td>Xpath root node</td>
<td>&lt;source_table_name&gt;</td>
</tr>
<tr>
<td>Expand node children</td>
<td>true</td>
</tr>
<tr>
<td>File retrieval method</td>
<td>HTTPS</td>
</tr>
<tr>
<td>File path</td>
<td>/&lt;source_table_name&gt;.do?XML</td>
</tr>
<tr>
<td>Server</td>
<td>&lt;instance name&gt;.service-now.com</td>
</tr>
<tr>
<td>User name</td>
<td>A user account on the remote instance. The username used cannot be an email address.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the same remote account.</td>
</tr>
</tbody>
</table>

4. Click Submit.
5. Click Test Load 20 Records to create the import set table and to ensure that your data source is functional.

Note: The 20 loaded records can't be transformed and are for testing purposes only.

Create a transform map

A transform map is a set of field maps that determine the relationships between fields in an import set and fields in an existing ServiceNow table, such as Incidents [incident] or Users [sys_user].

After creating a transform map, you can reuse it to map data from another import set to the same ServiceNow table.

1. Open the data source record that you just created.
2. In the Transforms related list, click New.
3. Populate all the usual fields and be sure to choose the proper **Target table**.
4. Submit the record.
5. Click **Auto map matching fields**.

**Add a field map for sys_id**
Add a field map to establish a relationship between the sys_id field in the source table (defined in the transform map) and the sys_id field in the target table.

1. Open the table transform map record you just created.
2. In the **Field Map** related list, click **New**.
3. Complete the form, using the following values
   - **Source field**: sys_id
   - **Target field**: Sys ID (You must do XML injection to make it work on older releases.)
   - **Coalesce**: Select the check box.

4. Click **Submit**.

**Add onBefore scripts to the transform map**
Create one onBefore transform map script to copy the sys_id of new records from the source to the target instance. Create a second onBefore transform map script to identify records on the target instance that have the same unique values but different sys_id values.

1. Open the table transform map record you created.
2. In the **Transform Scripts** related list, click **New**.
3. In the **When** field, select **onBefore**.
4. Enter the following script:
   ```javascript
   if (action == "insert") {target.setNewGuidValue(source.u_sys_id); }
   ```
5. Click **Submit**.
6. In the **Transform Scripts** related list, click **New**.
7. In the **When** field, select **onBefore**.
8. Enter the following **Script**:
   ```javascript
   /**
   * This script queries for a uniquely identifying value of the referenced record and then
   * updates the target reference field with the sys_id of the matching target record.
   * This sample assumes:
   * 1) The target table contains an assigned_to field which is a reference field.
   * 2) The reference field references the User [sys_user] table.
   * 3) You can use the email field to uniquely identify users. Alternatively you
   *    could use the user_name field.
   */
   var ref = new GlideRecord("sys_user"); //Replace sys_user with any reference table
   ref.addQuery("email", source.email); //Replace email with any unique field
   ref.query();
   if(ref.next()){
       target.assigned_to = ref.sys_id; //Replace assigned_to with any reference field
   }
   ```
9. Click **Submit**.

**Retrieving data from a CSV formatted file**

In this method, you import data from another instance using an HTTPS data source to return a CSV formatted file containing the rows to be imported.

This approach uses the Import Sets application to retrieve the data from the source and import it to the destination.

![CSV data source configuration](image)

**HTTPS Data Sources**

1. Create a new data source by navigating to **Import Sets > Data Sources** on the destination instance.
2. Provide the following field values:
   - **Import set table name**: Select a table.
   - **Type**: File
   - **Format**: CSV
• **File retrieval method**: HTTPS

  **Note:**
  If the **Server**, **File path**, **Username**, and **Password** fields are not visible when you select **HTTPS**, change the file retrieval method temporarily to **SCP** and enter this information. Remember to reset the **File retrieval method** to **HTTPS** after you enter these fields.

• **File path**: incident.do?CSV

  **Note:** To import specific change records, you can add qualifiers to the path. For example, the following path would return all active change records: 
  `incident.do?CSV&sysparm_query=active=true`

• **User name** and **Password**: Enter the user name and password for a valid user on the destination instance.

  3. Click the **Test load 20 records** related link to verify that the import is configured correctly.
  4. After setting up the data source, configure a standard transform map.

**System clone**

Use the System Clone application to copy everything in a database from one instance to another.

Cloning is typically used to copy a production instance to a pre-production instance to test changes. Cloning data comes from the most recent, nightly backup.
Clone process

In response to a clone request, the ServiceNow platform performs the following tasks:

1. Generates a file to preserve operational data on the target server.

   **Note:** This file contains the data preserved by data preservers.

2. Copies the database schema from the source instance to the target instance.

3. Creates tables in the target instance database using the source instance table definitions.
4. Copies data from the most recent nightly backup of the source instance to the target instance database.

Note: Certain exclusions are automatically large tables are normally excluded. These include audit, log, and email tables.

5. Briefly disables UI traffic and requests to the target instance server.

6. Displays the message **Clone in progress...** to any user accessing the target instance.

7. Restores operational data preserved from the target instance.

8. Runs any post-clone cleanup scripts on the target instance.

9. Briefly suspends all email functions on the target instance.

10. Queues an event to regenerate text indexes.

11. Enables UI traffic and requests to the target instance server.

During a clone, the target instance may be intermittently unavailable. After clone completion, you have up to 24 hours to contact Customer Service and Support and request a rollback of the target instance to its pre-clone state. You are notified when the rollback is complete.

**Clone to an instance on a different version**

The System Clone application can target an instance running a different instance version from the source.

A central web service controls clone processing and automatically modifies the target instance version to match the source instance version. This matching process starts up to 8 hours before the time specified in the **Date and time** field on the System Clone form. This web service also ensures that there is enough disk space on the target instance for the clone to proceed.

When cloning from a backup, the target instance does not need additional time to upgrade or downgrade. The ServiceNow platform performs any version changes during a brief window where the target instance is unavailable, after it copies data from the source instance backup.

**Clone from a backup**

The **ServiceNow** platform uses data from the most recent, nightly backup of the source instance when cloning. Backups that are used for cloning are a maximum of 36 hours old. System Clone begins the initial preparation, including selecting the latest backup to use, only at the date and time processing is scheduled to start.

If cloning from a source backup fails, the system uses the legacy clone engine instead. The legacy clone engine cannot preserve data from extended tables, relationships, hierarchies between tables, and dot-walked queries. You may want to restore the target instance from a backup and then reschedule the clone in such cases.

After cloning from a backup, the target instance is unavailable for several minutes before the clone is marked as complete in the source instance. If the source and target instances are on different versions of the **ServiceNow** platform, the target instance is modified to match the source instance version during this time.

When starting a clone from a backup, the date and time the backup was taken, as well as periodic progress messages, appear in the **Clone Log** related list.
System clone backup log

Clone over production instances

As long as the system property, `glide.db.clone.allow_clone_target` is TRUE, an instance can serve as a clone. Modifying data on the source instance during a clone can cause a data mismatch between records or duplicate record entries.

Request a clone

Request a clone to copy data from a production instance to a non-production instance or to copy data between non-production instances.

Role required: admin

The system uses data from the most recent, nightly backup of the source instance when cloning. Backups that are used for cloning are a maximum of 36 hours old. System Clone begins the initial preparation, including selecting the latest backup to use, only at the date and time processing is scheduled to start.

If cloning from a source backup fails, the system uses the legacy clone engine instead. The legacy clone engine cannot preserve data from extended tables, relationships, hierarchies between tables, and dot-walked queries. You may want to restore the target instance from a backup and then reschedule the clone in such cases.

For instances that use an Oracle database, see KB0538884 - System Clone Support for Oracle Customers.

You can automate cloning by scheduling it in the Options pane.

You cannot initiate a clone request when the source instance is in debug mode. If the source instance is in debug mode, contact Customer Service and Support to turn off debug mode before you submit a clone request.

1. Log in to the instance that you want to clone.
   This instance becomes the source instance of the clone request.
2. Create a clone target record for each target instance that you want to receive clone data.
3. Verify the list of tables that are excluded from cloning and add or remove tables to exclude from the target instance.
4. Verify the list of tables and system properties that you want saved on the target instance by data preservers. You can also create or modify data preservers, as needed.

   The legacy clone engine does not support data preservers for these records:
   - Tables that extend the Task table
   - Relationships
   - Hierarchies
   - Dot-walked queries

   If you are preserving any data that the legacy clone engine does not support, verify that there is a recent backup of the target instance available. If the clone-from-backup-process fails for any reason, you can restore the target instance from the backup.

5. Preserve any unpublished applications on the target instance.


7. Optional: Specify a predefined clone profile.

   A clone profile stores target and clone options. The clone profile automatically populates your clone request with your selected profile settings. See clone profiles for clone requests.

8. In the Target instance field, select the target instance that you want to receive the cloned data.

   Create a separate clone request for each target instance that you want to receive clone data.

9. In the Clone Scheduled Start Time field, select the time that you want the cloning to start.

   You can schedule multiple clone requests for the same source instance. For example, create one clone request to copy data to non-production instance A and another clone request to copy data to non-production instance B. The scheduling engine determines whether multiple clone requests against the same source instance can occur simultaneously or whether they must occur sequentially.

   The system verifies the scheduled start time and either accepts the date-time value that you selected or suggests an available date-time value. The validation process prevents scheduling conflicts with other automations using the same target instance.

10. In the Email upon completion field, enter your email address so that you can receive alerts after the cloning finishes, is canceled, or has an error.

11. Click the Options arrowhead so that it turns downward and use the following table to make appropriate selections in the Options pane.

   Clone options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exclude tables specified in Exclusion List</td>
<td>Prevents cloning records from the source instance specified in the System Clone &gt; Exclude Tables module. Use this option to create empty but usable tables on the target instance. By default, the system excludes tables for auditing, license usage, logging, and notifications. This option is selected by default.</td>
</tr>
<tr>
<td>Exclude audit and log data</td>
<td>Prevents cloning audit and log records from the source instance. Use this option to create empty but usable audit and log tables on the target instance. This option is selected by default.</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Exclude large attachment data              | Prevents the cloning of large attachments such as video files, image files, and other large binary file types. Use this option to exclude all common binary file types, regardless of file size. When selected, the clone also excludes attachments from the Attachments [sys_attachment] and Attachment Documents [sys_attachment_doc] tables that meet all these criteria.  
  • The attachment table_name value does not indicate that it is a small file. Small attachments have table-name values that start with ZZ_.  
  • The attachment data type value indicates that it is a large file such as an application or video.  
  • The attachment table_name is not one of these system tables: sys_certificate, ecc_agent_jar, ecc_agent_mib, sys_store_app, or invisible.sys_store_app.  
  This option is selected by default. |
| Preserve theme                             | Preserves the theme and CSS elements on the target clone. This option is selected by default.                                                                                                                    |
| Lock settings for this clone request       | If you use a clone profile, this option locks the settings and options at the time of the clone request. Any subsequent changes to the clone profile, regardless of when the clone runs, do not affect the clone request. This option is not selected by default. |
| Amount of data copied from large tables    | Clones the number of days of historical data from large source tables, including task, pa_scores, and metric_instance. By default, the target instance receives the latest 90 days of historical data from the source instance. |
| Preserve In Progress Update Sets           | Preserves update sets during the clone process. This option eliminates the need to export in-progress, global update sets before you initiate a clone. The default is none. You can select the latest 90 days to preserve the in-progress update sets during this time.  
  **Note:** Review and commit the update sets after the clone. |
| Preserve users and related tables          | Prevents users and user-related tables from being overwritten on the target clone. This option is not selected by default.                                                                                           |
| Clone frequency                            | Defines how often this target automatically receives clone data. By default, the clone frequency is set to None. For more information about scheduling cloning, see Schedule cloning.                                          |

12. Click **Submit**.

If there are no issues with the clone request, the system displays the Authenticate Target modal.

If your clone request preserves large tables, a warning message displays the large tables from your preserver list. You can cancel your clone request and remove the tables from your preserver list, or you can specify a reason and continue the clone request.
13. In the Username and Password fields, enter the username and password for an administrator account on the target instance and then click Authenticate.

14. Review the clone settings and click OK.

An email is sent to the supplied address after the clone finishes, is canceled, or has an error.

You can:

- Schedule automatic clonings.
- Cancel your clone request.
- View the cloning history of completed clonings.

Create a clone target

A clone target record specifies the instance URL and credentials used for cloning.

- User credentials for the target instance: provide credentials for a user with the admin role. Use a local, user account, not an LDAP or SSO user account. The target instance credentials must exist in the User [sys_user] table as a user record or as part of an LDAP integration. Clone requests cannot redirect authentication requests to a single sign-on identity provider.
- System property on target instance: verify the system property glide.db.clone.allow_clone_target is set to True. By default, this property is enabled on instances whose name ends in Dev, Test, Stage, UAT, or QA.
- IP Access controls on target instance: if the target instance uses IP range based authentication, it must allow the IP range 10.0.0.0/10.255.255.255 to communicate on a local network.
- Role required: clone_admin or admin.

1. Navigate to System Clone > Clone Targets.

2. Click New.

3. Enter the URL for the receiving instance (target).

The system validates the instance allows clone targets and that High Availability Cloning is active. Production and demonstration instances fail these validation checks.
4. Enter the basic authentication credentials for a user account with the admin role on the target instance.

![ServiceNow Instance](https://instance.service-now.com)

**Note:** You cannot request cloning multiple targets from the same source. Instead, make a separate request for each target.

The system validates the user credentials have admin access to the target instance.

5. Click **Submit**.

The system checks connectivity and validates the user credentials against the target instance.

### Exclude a table from cloning

Exclude a table to create an empty but usable table on the target instance.

The **System Clone > Exclude Tables** module lists the tables that are not copied during a system clone. By default, the system excludes tables for logging, auditing, notifications, workflow contexts, and license usage.

**Note:** Excluded workflow context data includes records stored in the `wf_context` table, and in related tables with names starting with a prefix of `wf_`. This also includes the workflow scheduler table. This prevents occurrence of workflow timer syncing issues that might take place due to the length of the cloning process if workflow contexts were included.

The system cannot exclude tables that extend the Task table and are also flattened into it as part of the table per hierarchy extension model. Since these extended tables are actually part of the same physical database table, the system clones the data when it clones the Task table. You can exclude tables that extend the Task table under two conditions. Either the system stores the tables in their own physical tables as part of the table per class extension model, or you exclude the Task table itself.

You can use wildcards to exclude several tables from cloning with one entry. For example, `sys_script.*` excludes all tables starting with `sys_script`.

**Note:** The wildcard has to include the dot `. ` before the asterisk.

To preserve the existing data on the target instance, see Create a data preserver. Data on tables that reference the table, such as business rules, is not excluded.

1. On the source instance, navigate to **System Clone > Exclude Tables**.
2. Click **New**.
3. Enter the table **Name**.
   Entering a parent table results in the clone process also excluding its child tables. For example, excluding the Task table would also exclude the Change, Incident, and Problem tables.
4. Click **Submit**.

## Data preservation on cloning target instances

You can use data preservers to protect data on the target instance from being overwritten. If you have custom applications, you must also manually preserve unpublished application content.

### Data preservers

Sometimes, it is necessary to preserve some data on an instance targeted for cloning. For example, if the target is a MID Server, you must not overwrite the MID Server [ecc_agent] table. Preserved data is stored on the target instance before cloning begins and is restored on the target instance after cloning.

**Warning:** You must define data preservers on the source instance. Defining them on the target instance does not preserve the data.

Data preservers typically preserve system settings and themes, such as:
- Instance-specific authentication settings
- Bookmark [sys_ui_bookmark]
- Recent Selection [sys_ui_recent_selection]
- User Preference [sys_user_preference]

**Note:** A clone does not support preserving data from a database view.

Do not use data preservers to transfer large sets of data, such as user groups. If you must preserve table data, such as users, groups, and roles, consider exporting the records to a file and importing them after cloning.

### Data preservers for Multi-SSO

The system automatically creates the necessary data preservers for cloning when you activate Multiple Provider Single Sign-On integration.

<table>
<thead>
<tr>
<th>Name</th>
<th>Table</th>
<th>Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate</td>
<td>X.509 Certificates [sys_certificate]</td>
<td>None</td>
</tr>
</tbody>
</table>
### Core Instance Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Table</th>
<th>Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>System Property [sys_properties]</td>
<td>• [OR] [Name] [is one of] [glide.authenticate.external, glide.authenticate.external.logout_redirect]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• [OR] [Name] [starts with] [com.snc.integration.saml_esig]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• [OR] [Name] [is one of] [glide.smtp.port, glide.smtp.auth, glide.smtp.encryption]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• [OR] [Name] [starts with] [glide.authenticate.multisso]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• [OR] [Name] [is] [glide.authenticate.sso.redirect.idp]</td>
</tr>
</tbody>
</table>

**Note:** The properties `glide.smtp.port`, `glide.smtp.auth`, and `glide.smtp.encryption` are deprecated.

### Digest Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Table</th>
<th>Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digest Properties</td>
<td>Digest Properties [digest_properties]</td>
<td>None</td>
</tr>
</tbody>
</table>

### Identity Providers

<table>
<thead>
<tr>
<th>Name</th>
<th>Table</th>
<th>Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Providers</td>
<td>Identity Providers [sso_properties]</td>
<td>None</td>
</tr>
</tbody>
</table>

### SAML2 Update1 Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Table</th>
<th>Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML2 Update1 Properties</td>
<td>SAML2 Update1 Properties [saml2_update1_properties]</td>
<td>None</td>
</tr>
</tbody>
</table>

**Note:** Although you can modify these data preservers, it is good practice not to. The Digest Properties [digest_properties], Identity Providers [sso_properties], and SAML2 Update1 Properties [saml2_update1_properties] tables are required for multiple source, single sign-on (SSO) to function properly. If multiple source, single sign-on is disabled on the target instance, you can safely remove all three data preservers. Remove them at the same time, as the system terminates the clone with an error message when you attempt to clone with one or two of these tables being preserved.

---

### Data preservers for SAML

Preserving SAML SSO-related settings can prevent the target instance from using the wrong issuer and audience parameters when making authentication requests to your IdP. To preserve SAML settings, create data preservers for the following tables:

- System Property [sys_properties]: to preserve SAML properties.
- X.509 Certificates [sys_certificate]: to preserve SAML certificates.
- User [sys_user]: to preserve SAML users.

You also need to preserve properties and users that are involved in SAML.

### Preservation of unpublished applications

You cannot use data preservers to save unpublished applications. Instead, application developers must choose how they want to preserve unpublished applications.
The cloning process does not preserve version differences for applications in development. Instead, the system clone only copies the application version installed on the source instance onto the target instance. If the target instance had a development version of the same application, the application will be editable after the clone, but it will be at whatever version was installed on the source instance. If the application was missing from the source instance, the cloning process deletes the application from the target instance.

**Create a data preserver**

Data preservers maintain specified data on a target instance.

Role required: clone_admin or admin

Sometimes, preserving certain data on a target instance is desirable. For example, when using a MID Server, you can avoid overwriting the MID Server [ecc_agent] table. Preserved data is stored in a dynamically generated list on the target instance before the clone and restored on the target instance after the clone is complete. You define data preservers on the source instance.

Data preservers are primarily intended to preserve system settings and themes, such as instance-specific authentication settings. Do not use data preservers to transfer large sets of data, such as user groups. If you must preserve table data such as users, groups, and roles, consider exporting the records to a file and importing it after the clone is complete.

Consider whether to preserve the data in the following tables.

- Bookmark [sys_ui_bookmark]
- Recent Selection [sys_ui_recent_selection]
- User Preference [sys_user_preference]

If you set a data preserver on a table where the source instance has more records than the target instance, the data preserved on the target instance also includes the additional records from the source instance.

For example, assume that the data preserver is already in place.

- In the source instance, the sys_temp table contains 100 records.
- In the target instance, the sys_temp table contains 20 records.

After the clone, the sys_temp table in the target instance contains 100 records.

- The 20 records in the target sys_temp table are preserved successfully (per the data preserver specification). These records were part of the 100 records in the source sys_temp table.
- The source sys_temp table brings over the remaining 80 records to the target sys_temp table.

To resolve this issue and to preserve only the records in the target table, create an exclude table record for the target table, in addition to setting the data preserver on the source table.

### Important: Configure preservers on the source instance.

1. On the source instance, navigate to **System Clone > Preserve Data**.
2. Click **New**.
3. Enter the table label as the **Name**, for example, User Preference for the [sys_user_preference] table. The data preserver must have a table name or it cannot be submitted.
4. Select the **Table** to be preserved.
   The data preserver must have a table selected or it cannot be submitted.
5. Select the **Theme** check box if the data being preserved is a UI property.
6. Define the data to be preserved using the **Condition Builder**.

You can use conditions to define particular records you want to preserve during a clone. For example, to only preserve particular system properties, you can add conditions for each property name you want to preserve.

**Note:** The condition to match regular expressions [match regex] is no longer supported.

**Warning:** If the clone from backup fails for some reason, the clone process fails over to the legacy clone engine. The legacy clone engine cannot preserve data from extended tables, relationships, hierarchies between tables, and dot-walked queries. You may want to reschedule a system clone or manually transfer data in such cases.
7. Click **Submit**.

    If you want to delete the data preserver later, make sure not to modify or delete the following data preserver records:
    
    - Core Instance Properties
    - Semaphores
    - Email Accounts

*Preserve SAML properties*

If you want a clone target instance to keep its existing SAML integration, you must edit the **Core Instance Properties** data preserver to include the SAML properties.

Role required: admin

1. Navigate to **System Clone > Preserve Data**.
2. Select **Core Instance Properties**.
3. Add the following **Conditions**.

   - [OR] [Name] [is one of] [glide.authenticate.external, glide.authenticate.external.logout_redirect, glide.authenticate.failed_requirement_redirect]
   - [OR] [Name] [starts with] [glide.authenticate.sso.saml2]
   - [OR] [Name] [starts with] [com.snc.integration.saml_esig]
<table>
<thead>
<tr>
<th>Name</th>
<th>Condition</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>is</td>
<td>glide.sys.schedulers</td>
</tr>
<tr>
<td>Name</td>
<td>starts with</td>
<td>glide.db</td>
</tr>
<tr>
<td>Name</td>
<td>is</td>
<td>glide.ui.max.transaction</td>
</tr>
<tr>
<td>Name</td>
<td>starts with</td>
<td>glide.email</td>
</tr>
<tr>
<td>Name</td>
<td>starts with</td>
<td>glide.op3</td>
</tr>
<tr>
<td>Name</td>
<td>is</td>
<td>instance.id</td>
</tr>
<tr>
<td>Name</td>
<td>is</td>
<td>instance.name</td>
</tr>
<tr>
<td>Name</td>
<td>starts with</td>
<td>glide.installation</td>
</tr>
<tr>
<td>Name</td>
<td>is one of</td>
<td>glide.authenticate.external, glide.authenticate.external.logout_redirect, glide.authenticate.failed_requirement_redirect</td>
</tr>
<tr>
<td>Name</td>
<td>starts with</td>
<td>glide.authenticate.sso.s</td>
</tr>
<tr>
<td>Name</td>
<td>starts with</td>
<td>com.snc.integration.ssan</td>
</tr>
</tbody>
</table>
Note: Ensure the Theme check box is cleared so these properties are preserved regardless of whether you preserve the instance theme.

4. Click Update.

Preserve unpublished applications during a system clone
Application developers must manually save a copy of each application currently in development prior to cloning over their development instance.

- Role required: admin
- Write access to the application record
- A source control repository

The cloning process does not preserve version differences for applications in development. Instead, the system clone only copies the application version installed on the source instance onto the target instance. If the target instance had a development version of the same application, the application will be editable after the clone, but it will be at whatever version was installed on the source instance. If the application was missing from the source instance, the cloning process deletes the application from the target instance.

1. Use one of these actions to preserve the application on the clone target instance.

<table>
<thead>
<tr>
<th>Version differences between instances</th>
<th>Action to take</th>
</tr>
</thead>
<tbody>
<tr>
<td>The application version on the clone target instance is different than the source instance version.</td>
<td>Export each application from the clone target instance. Choices include:</td>
</tr>
<tr>
<td></td>
<td>- (Recommended) Link each application to a source control repository.</td>
</tr>
<tr>
<td>The application is only available on the clone target instance.</td>
<td></td>
</tr>
<tr>
<td>The application version on the clone target instance is the same as the source instance.</td>
<td>None. The system clone process will copy this application version onto the target instance during the clone.</td>
</tr>
</tbody>
</table>

2. Request a system clone of the source instance over the target instance.
For example, clone your production instance over your development instance.

3. After the clone process finishes, log in to the clone target instance.

4. If you saved each application to a source control repository, use one of these actions to retrieve them from the source control repository.

Retrieve applications from a source control repository

<table>
<thead>
<tr>
<th>Application installation state</th>
<th>Action to take on clone target</th>
</tr>
</thead>
<tbody>
<tr>
<td>The application was previously installed on the source instance.</td>
<td>Apply remote changes from source control repository.</td>
</tr>
<tr>
<td>The application was never installed on the source instance.</td>
<td>Import the application from source control repository.</td>
</tr>
</tbody>
</table>
5. If you saved each application to an update set, use one of these actions to retrieve them from the update set.

**Retrieve applications from an update set**

<table>
<thead>
<tr>
<th>Application installation state</th>
<th>Action to take on clone target</th>
</tr>
</thead>
<tbody>
<tr>
<td>The application was previously installed on the source instance.</td>
<td>a. Delete the application version cloned from the source instance.</td>
</tr>
<tr>
<td></td>
<td>b. Load the update set containing the current application version.</td>
</tr>
<tr>
<td>The application was never installed on the source instance.</td>
<td>Load the update set containing the current application version.</td>
</tr>
</tbody>
</table>

The applications previously in development are available for further development on the clone target instance.

**Preserve the Marketing Events application**

Suppose your company previously created version 1.0 of a custom application called Marketing Events. You have already published version 1.0 of the Marketing Events application to the application repository and installed it on your production instance.

Over time, users have submitted enhancement requests for the application, and you decide to develop version 2.0 of the Marketing Events application on a non-production instance to address these requests. As development nears completion, you want to update your non-production instance to the latest copy of production for some comprehensive testing.

Since you previously used a source control integration to develop version 1.0 of the Marketing Events application, you have already linked the Marketing Events application to a source control repository. You commit version 2.0 of the Marketing Events application to the source control repository.

You schedule a clone of the production instance over the development instance. After completion, you log in to the development instance and see that it has version 1.0 of the Marketing Events application, because that was the version installed on the source instance.

Since the application was already installed on the source instance, you apply remote changes from the source control repository to receive the latest application version. The development instance now has version 2.0 of the Marketing Events application available for further development and testing.

**Clone profiles for clone requests**

A clone profile enables you to store predefined target and clone options. The clone profile automatically populates your clone request with your selected profile settings.

**Clone profiles**

Navigate to **System Clone > Clone Profiles** to view your clone profiles. With a clone profile, you can:

- Create a profile with specific target instance and option settings, tables to exclude, data to preserve, and cleanup scripts to run
- Create a clone request directly from the clone profile
- Apply the clone profile to a clone request

You can create, edit, and delete clone profiles from the **Clone Profile** view. The system profile is a read-only clone profile that you can't delete. It shows a predefined list of table exclusions, data preservers, and cleanup scripts. This list is based on the plugins that your instance contains.
After you create a clone profile, you can select the **Make Default** option so that the clone is referenced as the clone profile when you request a clone.

**Cancel a clone**

You can cancel requested, scheduled, and active clones without negatively impacting system stability or usability. Canceling a clone restores the target instance to the pre-clone state, retaining all original data.

Role required: admin
Active system clone

After starting a clone, the **Clone Log** and **Database Table Clones** related lists appear on the form. These related lists show general log messages, and the details of individual tables respectively.

The duration a clone remains active varies upon the amount of data being cloned, and whether the source and target instance are in the same physical location. If a clone takes longer than anticipated, ServiceNow Technical Support can identify additional details about the clone progress.

1. Navigate to **System Clone > Live Clones > Active Clones**.
   - The system displays the list of currently active clones.
2. Select the clone you want to cancel.
   - The system displays the System Clone record.
3. From Related Links, click Cancel Clone.
   The Cancel Clone modal displays.

4. In Specify Reason, select a reason for the cancellation and click OK, or select Others, enter a reason in the text box and click OK.
   The system stops any current clone activities and sets the State to Canceled.

If you want to restart a canceled clone, you must create a new clone request.

Schedule cloning

You can use System Clone to schedule automatic clonings, which is the easiest way to keep your cloned instances up to date.

Role required: admin

Instead of manually cloning instances, you can schedule clonings that happen automatically. You create a cloning schedule in the same interface you use to create a clone. This topic assumes that you created a clone but not a cloning schedule for it.

1. Click System Clone > Active Clones > <one-of-your-clones>.
2. Click the **Options** arrowhead so it turns downward.

   The **Options** panel appears.

3. Enter values in the following fields to schedule automatic clonings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clone frequency</td>
<td>Defines how often this target automatically receives clone data.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>No. of occurrences</td>
<td>Specify the number of automatic clonings. The maximum value you can enter depends on the value selected for the clone request in the</td>
</tr>
<tr>
<td></td>
<td>Clone Frequency field. The following are the maximum value for each selected the clone frequency:</td>
</tr>
</tbody>
</table>

4. Click **Submit**.
   The system displays the Authenticate Target modal.
5. Enter the **Username** and **Password** for an administrator account on the target instance and click **Authenticate**.
   The System Clone form displays for the target clone.
6. To see the cloning schedule for this target, click the **Recurring Clones** tab.
   Each line in the list shows a separate, scheduled cloning session.
7. To see log messages for past clonings on this target, click the **Clone Log** tab.
8. To see cloning schedules for all the clones in the system, click System Clone > Live Clones > Clone History.
   The **System Clones** page lists all the cloning instances in the system along with their scheduled clonings.

**Modify cloning schedules**

You can cancel scheduled clonings but not modify them.

Role required: admin

This topic assumes that you have a cloning schedule that you want to modify. Cloning schedules cannot be modified. Instead, you have to cancel scheduled clonings and create a new cloning schedule.

1. Click **System Clone > Active Clones > <one-of-your-clones>**.
   The System Clone record opens for your cloning instance.
2. To delete one or more scheduled clonings, on the **Recurring Clones** tab, select the check box next to the row(s) you want to cancel and on **Actions on selected rows**, click **Delete**.
3. If you deleted all future clonings, you can create a new cloning schedule.
   You cannot create more than one cloning schedule for a target instance.
4. To stop a cloning that is already in progress, under **Related Links**, click **Cancel Clone**.
   The system stops any current cloning activities and sets the **State** to **Canceled**. Future, scheduled clonings are not deleted.

**View clone status**

You can view the status of a clone to make sure the cloning process isn't stuck.

Role required: admin

1. Navigate to **System Clone > Live Clones > Active Clones**.
   The system displays the list of currently active clones.
2. Select the clone you want the status of.
   The system displays the System Clone record of that clone.
3. Under **Related Links**, click **Check Clone Status**.
   The system updates the **State** field and produces a log entry in the **Clone Log** that shows the status of the clone.

   ![Clone Log](image)

   If a cloning status is failed, you might **roll back the cloning** and **schedule a new cloning**.

**View clone history**

You can view the status and history of any system clone request.
Role required: clone_admin or admin
The System Clone [clone_instance] table stores records for all previously and currently scheduled clones.

1. **Navigate to System Clone > Live Clones > Clone History.**

   Clone history also displays the **State** for current and past clones. Clones in the **Draft** state do not appear on the Clone History table.

<table>
<thead>
<tr>
<th>Clone state</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requested</td>
<td>The clone was requested and is awaiting approval.</td>
</tr>
<tr>
<td>Scheduled</td>
<td>The clone is ready to begin at the scheduled time and date.</td>
</tr>
<tr>
<td>Active</td>
<td>The clone is currently running.</td>
</tr>
<tr>
<td>Completed</td>
<td>The clone completed successfully.</td>
</tr>
<tr>
<td>Canceled</td>
<td>A user canceled the request.</td>
</tr>
<tr>
<td>Hold</td>
<td>The server rejected the clone request. This can happen either because the clone was not ready to proceed by the scheduled time or because additional clone requests were submitted before the first one completed.</td>
</tr>
<tr>
<td>Error</td>
<td>The clone encountered an error while running. Contact technical support for help resolving this issue.</td>
</tr>
<tr>
<td>Draft</td>
<td>The clone is scheduled to be created. This state never appears in the Clone History table.</td>
</tr>
</tbody>
</table>

2. **Select a System Clone record to view its history.**

**Roll back a clone**

Return a clone target to its state before the latest cloning. Roll back cloning if something went wrong in the cloning process.

Role required: admin

Rollbacks remove the latest cloning updates on a cloning target. You can only roll back the latest cloning updates. Rollbacks must occur no more than seven days after the cloning.

1. **Navigate to System Clone > Live Clones > Clone History.**

2. **Select the clone to roll back.**

4. In Specify Reason, select a reason for the rollback and click OK, or select Others, enter a reason in the text box and click OK.

The system rolls back the clone and sets the State to Rollback Requested, and, if successful, to Rolled Back, or, if unsuccessful, to Rollback Failure.

You can retry a rollback but if you get repeated failures, contact ServiceNow Customer Support.

The instance contains the same data it had before the clone was applied.

Post-clone cleanup scripts

Cleanup scripts automatically run on the target instance after the cloning process finishes. Use cleanup scripts to modify or remove bad data. Cleanup scripts run after data preservers and the clone are complete.

You can add new post-cloning scripts on the source instance to perform any action that can normally be accomplished through script includes or business rules. To add a script, navigate to System Clone > Clone Definition > Cleanup Scripts and click New.

You can make post-clone scripts active or inactive to control whether these scripts run or do not run. You can also set an order number on each script, which enables you to set the order that the active scripts run, with lower numbers having a higher priority.
The following post-clone cleanup scripts perform various actions on the target instance.

**Post-clone cleanup scripts**

<table>
<thead>
<tr>
<th>Script</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bad MID Server credentials after clone</td>
<td>Runs a script include called BadMIDCredentialAfterClone on a cloned instance to detect <strong>bad MID Server user credentials</strong>. This script include creates scheduled jobs that log MID Servers in the <strong>Down</strong> state to the MID Server Issue [ecc_agent_issue] table after an instance clone.</td>
</tr>
<tr>
<td>Script</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Clear scheduled job node association</td>
<td>Resets any scheduled jobs that were active on the source instance to the <strong>Ready</strong> state. This script also clears the value of the <strong>System ID</strong> and <strong>Claimed by</strong> fields on all scheduled jobs.</td>
</tr>
<tr>
<td>Configure Email Accounts</td>
<td>Migrates email accounts that existed on the source instance to the target instance if they are not enabled there. This script also migrates the email properties to the target instance.</td>
</tr>
<tr>
<td>Disable emails</td>
<td>Disables email on the target instance. A default data preserver maintains other email settings from the target instance.</td>
</tr>
<tr>
<td>Install deactivated plugin</td>
<td>Enables the Domain Separation plugin for instances that use this feature.</td>
</tr>
<tr>
<td>Regenerate all text indexes</td>
<td>Rebuilds text indexes on the target instance after a clone. Text indexes are not cloned from the source to the target instance.</td>
</tr>
<tr>
<td>Schedule drop backup tables</td>
<td>Schedules the deletion of the data that is contained in the target instance database prior to the clone. This original data is preserved for 24 hours following a clone to enable you to roll back an instance to the pre-clone state. If the target instance is downgraded as part of the clone, backup data is not available.</td>
</tr>
</tbody>
</table>

**Database rotation**

Database rotation involves managing table size growth and archiving old data.

Data within an instance grows quickly, and as these tables grow in size they require management. Database Rotation preserves instance performance and averts risk associated with querying growing data sets utilizing three techniques. These techniques are based on the concept of managing large quantities of data by separating whole sets into individual tables. After this task is performed, each technique handles data in a different manner:

- Table Rotation works by rotating among a small set of tables, and deleting and reusing the old tables for new data.
- Table Extension works by periodically starting a new table and allowing old tables to be easily archived and removed from the system.
- Table Sharding works by enabling records to be grouped in a single table by document ID.

**Table rotation plugins**

- **Database Rotations Plugin** activates Table Rotation and Extension without any tables automatically included (com.snc.db.rotation)
- **Database Rotations Default Tables Plugin** applies Table Rotation and Extension to specific tables (com.snc.db.rotation_default_tables)
Database Rotation

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Tables applied to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table Rotation</td>
<td>syslog, sys_querystat, ecc_queue, ecc_event, cmdb_metric, sysevent</td>
</tr>
<tr>
<td>Table Extension</td>
<td>sys_audit, sys_email</td>
</tr>
</tbody>
</table>

Reference values converted to strings

Archived data is stored as a flat file with no reference fields to other tables. The archive process converts any references to other tables to string values.

In the case of a reference field, the string uses the display value such as the caller's user name. For example, the Caller reference field in an incident would display the string ITIL User. If the reference was a document ID and the archive rule included the option to archive related document IDs, then the string is the document ID of the related record.

It is important to note that archive records do not receive any future changes to referenced values. For example, if you change the user name for "John Smith" to "John A Smith", all active incident records automatically show the caller as "John A Smith" because of the reference between the Incident and User tables. However, all archived incident records display the user name that existed at the time of the archive. Any incident for "John Smith" continues referencing this user. Likewise, if you delete a user from the system, current incidents no longer display the deleted user as a caller. However, there can be archived incidents that still display the string "John Smith" as the user because the user existed at the time of the archive.

Table rotation and extension

The System Definition Table Rotation module allows you to define a new table rotation, a new table extension, a new table shard, or modify an existing one.
Table rotation groups

- **Name**: auto-generated from table name
- **Duration**: overall time parameter for function
- **Initialized**: sets function as active (true) or inactive (false)
- **Rotations**: number of tables to be created within Duration
- **Type**: indicates Extension (archiving), Rotation (deletion), or Shard (doc ID) functionality

When you define a new rotation, a schedule is created and new data is subsequently written to one of the tables in the rotation group. You'll notice the that the group includes the original table plus a number of additional tables. Be aware that deleting a rotation will delete the additional tables and all the data, therefore the rotation should not be deleted if the data is needed.

See these topics for more information on managing tables:
- **Table Rotation**
- **Table Extension**

**Activate database rotation**

For new instances, database rotation is active by default. If you are upgrading from a previous version, you can activate the Database Rotations plugin if it is not already active.

**Note**: Deployment of this plugin should be executed in partnership with a ServiceNow representative.

If it is not already active, you can activate the Database Rotations plugin if you have the admin role.

1. Navigate to **System Applications > All Available Applications > All.**
2. Find the plugin using the filter criteria and search bar.

   You can search for the plugin by its name or ID. If you cannot find a plugin, you might have to request it from ServiceNow personnel. For more information, see Request a plugin.

3. Click **Install**, and then in the Activate Plugin dialog box, click **Activate**.

   **Note:** When domain separation and delegated admin are enabled in an instance, the administrative user must be in the **global** domain. Otherwise, the following error appears: **Application installation is unavailable because another operation is running:** Plugin Activation for <plugin name>.

Do not activate the **Database Rotations Default Tables** plugin. Instead, specify the tables manually, after consulting a ServiceNow representative.

### Domain separation and Data Management

Domain separation is supported in Data Management. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can control several aspects of this separation, including which users can see and access data.

**Support level: Basic***

- There is business logic to ensure data goes into the proper domain for the application’s service provider use cases.
- In the application, the user interface, cache keys, reporting, rollups, aggregations, and so on, all consider domain at run time.
- The owner of the instance needs to be able to set up the application to function normally across multiple tenants.

Use case: As a service provider when I use chat to respond to a tenant-customer’s message, the client must be able to see my response.

### Integration with third-party applications and data sources

ServiceNow integrates with many third party applications and data sources.

The most common integrations are with CMDB, Incident Management, Problem Management, Change Management, User Administration, and Single Sign-on. A variety of techniques can be used, most notably Web Services, JDBC, LDAP, Excel, CSV, and Email, as well as any industry standard technologies that use SOAP, REST, or WSDL. Additionally, API and command-line integrations can be done using a MID Server. ServiceNow has performed the following integrations with enterprise systems and platforms.

This podcast offers additional information on integrations.

### Technologies

The ServiceNow platform is based on service-oriented architecture (SOA), in which all data objects can use web services to access bi-directional data-level integration. The interface is also direct and dynamic because all modifications to existing objects and all new objects are automatically published as a Direct Web Service. A more indirect web service creation and usage can be achieved through Mapped Web Service where a transform map is used to gather incoming web service data into the final targeted tables. Finally, an advanced Scripted Web Service technique is available for defining process-based web services, where data is irrelevant, but serves more as a trigger for a process or a composite of actions that execute at the server.
Additionally the platform offers a rich interface for loading external data using import sets. Using this feature, you can load from various data sources such as HTTPS, FTPS, and SCP using file formats such as XML, CSV, and Microsoft Excel XLS files. Information can also be pulled from a data source using a direct JDBC connection, provided the network connectivity allows.

Information can be pulled from the platform to an external platform using an ODBC Driver.

Forms, lists, and reports on the platform can be accessed directly using a URL, which facilitates integration on the UI level between two or more web applications.

A handful of single sign-on technologies is identified and implemented out of the box to allow fast integration with your portal, however, the technique is customizable in a script to allow for flexibility in the different SSO environments our customers have.

### Integration between ServiceNow Instances

There are times when you find you need to perform a specific integration between your instance and another ServiceNow instance. Instance-to-Instance integrations are a snap because all of the integration points exist between the two instances.

### Integration options

Nearly all ServiceNow customers obtain additional value by integrating with third-party applications.

ServiceNow customers have the following options for integrating with third-party applications.

- Activate a ServiceNow provided integration.
- Install a certified integration from the ServiceNow Store.
- Install an integration from Share.
- Contact your sales representative for available custom-built integrations.
- Build your own custom integration using the platform's integration interfaces.

**Note:** Certified integrations have passed a set of interoperability, security, and performance test criteria defined by ServiceNow.

### ServiceNow provided integrations

ServiceNow provides many integrations as part of the platform.

These integrations are considered part of the platform and are provided at no additional charge.

<table>
<thead>
<tr>
<th>Integration</th>
<th>Type</th>
<th>Integration Point</th>
</tr>
</thead>
<tbody>
<tr>
<td>Altiris (version 6.5)</td>
<td>MID Server</td>
<td>CMDB</td>
</tr>
<tr>
<td>Google Maps</td>
<td>Web services</td>
<td>Varies</td>
</tr>
<tr>
<td>Google Custom Search</td>
<td>Web services</td>
<td>Knowledge</td>
</tr>
<tr>
<td>Integration — IBM Watson</td>
<td>Web services</td>
<td>Varies</td>
</tr>
<tr>
<td>Conversation Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft SMS / SCCM</td>
<td>MID Server</td>
<td>CMDB</td>
</tr>
<tr>
<td>Verizon eBonding</td>
<td>Web services</td>
<td>Incident</td>
</tr>
</tbody>
</table>
Set up Google Maps API

You enable the geolocation feature using the appropriate entries from a Google Maps API for Business license, or a Google Maps Javascript API Key.

Role required: admin

You can generate maps using basic JavaScript, and they are flexible enough to display even the most complicated of queries. These maps use standard Google Maps API for Business or Google Maps Javascript API Key mapping features, including various link types to records in your instance. Use of this feature requires installation of the Google Maps plugin.
1. Google Maps APIs for Business licenses are no longer available from Google, so, depending on whether you have an existing license, use one of the following procedures.

<table>
<thead>
<tr>
<th>Existing Google Maps API for Business license available?</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existing license available</td>
<td>a. In the System Properties &gt; Google Maps property form:</td>
</tr>
<tr>
<td></td>
<td>• In the google.maps.client field, enter the Client ID for your organization. This ID is from Google and starts with gme-, such as gme-mycompanyname.</td>
</tr>
<tr>
<td></td>
<td>• In the google.maps.private.key field, enter the private key for Google Maps API for Business. An example of an encoded key is vNIXE0xscrmjlyV-12Nj_BvUPaw=. The Now Platform® requires this key to retrieve accurate driving time estimates from Google for some Geolocation features.</td>
</tr>
<tr>
<td></td>
<td>• Fill out the remaining values on the form.</td>
</tr>
<tr>
<td></td>
<td>b. Configure your maps using the property definitions from the table.</td>
</tr>
</tbody>
</table>

**Note:** See the Getting Started Guide on the Google website for details on obtaining a key, using the API, and relevant terms of service.
Existing Google Maps API for Business license available?

<table>
<thead>
<tr>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Obtain a Google Maps Javascript API Key from Google.</td>
</tr>
<tr>
<td>b. In the <strong>System Properties &gt; Google Maps</strong> property form, enter the API key into the <code>google.maps.key</code> field. Geolocation in the Now Platform® uses the API Key, which Google Maps also uses for Geolocation and map view billings.</td>
</tr>
<tr>
<td>c. Fill out the remaining values on the form.</td>
</tr>
<tr>
<td>d. Configure your maps using the property definitions from the table.</td>
</tr>
</tbody>
</table>

To learn more about Google Maps API for Business, and Google Maps Javascript API Key, see [https://developers.google.com/maps/gmp-get-started](https://developers.google.com/maps/gmp-get-started).

2. After you complete and save the configuration, create Map pages, or use the default pages included with the plugin.

Map pages define what data appears on the map, and the appearance of the links. For a tutorial on how to view all of the markers that link to your records, see the [Display Map Markers on Google Maps](https://community.service-now.com/) blog post on the Now Community.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>google.maps.auto_close</td>
<td>If true, automatically closes a map information window before opening a new one.</td>
</tr>
<tr>
<td></td>
<td>• Type: true/false</td>
</tr>
<tr>
<td></td>
<td>• Default value: true</td>
</tr>
<tr>
<td></td>
<td>• Location: <strong>System Properties &gt; Google Maps</strong></td>
</tr>
<tr>
<td>google.maps.client</td>
<td>Client ID for Google Maps API for Business.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: gme-servicenow</td>
</tr>
<tr>
<td></td>
<td>• Location: <strong>System Properties &gt; Google Maps</strong></td>
</tr>
<tr>
<td>google.maps.private.key</td>
<td>Private key for Google Maps API for Business. This key activates the geolocation feature, which locates users in the system precisely, using data from their mobile devices.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: empty</td>
</tr>
<tr>
<td></td>
<td>• Location: <strong>System Properties &gt; Google Maps</strong></td>
</tr>
<tr>
<td>google.maps.version</td>
<td>Version number of the current installation of Google Maps API for Business.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: current version number</td>
</tr>
<tr>
<td></td>
<td>• Location: <strong>System Properties &gt; Google Maps</strong></td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>google.maps.key</td>
<td>Google Maps API for Business or Google Maps Javascript API Key that ties to the URL of the server. This key authorizes development use of Google Maps API.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: empty</td>
</tr>
<tr>
<td></td>
<td>• Location: <strong>System Properties &gt; Google Maps</strong></td>
</tr>
<tr>
<td>google.maps.latitude</td>
<td>Starting latitude of the map. This value determines the starting position displayed in Google Maps.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: 36.008522</td>
</tr>
<tr>
<td></td>
<td>• Location: <strong>System Properties &gt; Google Maps</strong></td>
</tr>
<tr>
<td>google.maps.longitude</td>
<td>Starting longitude of the map. This value determines the starting position displayed in Google Maps pages.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: -95.221764</td>
</tr>
<tr>
<td></td>
<td>• Location: <strong>System Properties &gt; Google Maps</strong></td>
</tr>
<tr>
<td>google.maps.max_items</td>
<td>Maximum number of items to display on the map.</td>
</tr>
<tr>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 500</td>
</tr>
<tr>
<td></td>
<td>• Location: <strong>System Properties &gt; Google Maps</strong></td>
</tr>
<tr>
<td>google.maps.table</td>
<td>Table used by the map. The table needs the following fields: name, longitude, latitude.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: cmn_location</td>
</tr>
<tr>
<td></td>
<td>• Location: <strong>System Properties &gt; Google Maps</strong></td>
</tr>
<tr>
<td>google.maps.zoom</td>
<td>Starting zoom level of the map (1 is the lowest)</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: 4</td>
</tr>
<tr>
<td></td>
<td>• Location: <strong>System Properties &gt; Google Maps</strong></td>
</tr>
</tbody>
</table>

3. **Perform these configurations:**
   a) Navigate to **System Properties > All.**
   b) Set values for these system properties:

<table>
<thead>
<tr>
<th>System property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>google.maps.refresh.latlong.duration</td>
<td>Number of days after which the location details are updated.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The maximum value is 30.</td>
</tr>
<tr>
<td>System property</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>google.maps.refreshlatlong.record_count_per_table</td>
<td>Maximum number of records in a table that can be processed using the scheduled job in one refresh.</td>
</tr>
</tbody>
</table>

c) Specify the tables that store the location details in the Map Coordinates Refresh Configuration [cmn_coordinate_refresh_config] table.

d) If there are no fields to track when the coordinates are last retrieved in your tables:

1. Create the coordinates_retrieved_on field of the type Date/Time in your tables.
2. Ensure that the value of the field that tracks time when the coordinates are last retrieved, is populated correctly in the Map Coordinates Refresh Configuration [cmn_coordinate_refresh_config] table. Refer to the sample fix script Update coordinates updated on field to update values in the coordinates_retrieved_on field.

e) Navigate to System Definition > Scheduled Jobs.

f) Open the record, Refresh Latitude Longitude info of Records.

g) Select the Active check box.

h) Specify the frequency at which the location details should be refreshed by providing frequency details in Run and Repeat Interval.

**Note:** Ensure that you refresh the location details at least once every 30 days.

---

**Request Google custom search integration**

The Google Custom Search Integration plugin is available by request.

Role required: admin

There are two ways to request a plugin:

- Access the Now Support Service Catalog directly by clicking Service Catalog > Activate Plugin on Now Support.
- Access the Now Support Service Catalog through the All Applications page on your instance by following these steps.

1. Navigate to System Applications > All Available Applications > All.
2. On the All Applications page, click **Request Plugin** to open the Request form on HI.
3. On Now Support, select the redirect link to access the Now Support Service Portal Service Catalog.

<table>
<thead>
<tr>
<th>Activate Plugin</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>In order to enhance the user experience, we have redesigned Activate a Plugin service catalog. Please use the new HI Service Portal 'Activate a Plugin' service catalog item. You can also use Manage Instances page on Service Portal to Activate a Plugin.</td>
<td></td>
</tr>
<tr>
<td>Take me to the HI Service Portal Activate a Plugin Service Catalog.</td>
<td></td>
</tr>
</tbody>
</table>

4. On the form, fill in the fields.

**Activate Plugin request form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Instance</td>
<td>Instance on which to activate the plugin.</td>
</tr>
<tr>
<td>Plugin Name</td>
<td>Name of the plugin to activate.</td>
</tr>
<tr>
<td>Specify the date and time you would like this plugin to be enabled</td>
<td>The date and time must be at least two business days from the current time.</td>
</tr>
</tbody>
</table>

**Note:** Plugins are activated in two batches, once in the morning and once in the evening, on every business day in the US Pacific time zone. If the plugin must be activated at a specific time, enter the request in the Reason/Comments field.

| Reason/Comments | Information that would be helpful for the ServiceNow personnel who are activating the plugin. For example, if you need the plugin activated at a specific time instead of during one of the default activation windows, specify that in the comments. |

5. Click Submit.

**Microsoft SCCM integration**

The Microsoft SCCM integration is a one direction import of SCCM data into the ServiceNow's Configuration Management Database (CMDB).

Scheduled imports bring relevant SCCM data into the ServiceNow instance from an SQL Server database and map it to tables in the CMDB. You can configure either a full or incremental data import. The import is achieved using a JDBC connection via the MID Server. The integration keeps the ServiceNow CMDB synchronized with the SCCM SQLServer database, so that only relevant data is imported from the SCCM database to the CMDB. The SCCM database is considered an authoritative source and is not written to.
Supported versions

These are the plugins for the currently supported SCCM versions, all of which support Asset Intelligence and Incremental Software Reconciliation:

- Microsoft SCCM 2007
- Microsoft SCCM 2012 v2
- Microsoft SCCM 2016

Note: If you upgrade your instance to a version of the Now Platform that does not provide support for your version of SCCM, you can continue to use that version. However, all new instances require the use of a supported SCCM version.


Service Graph connector for Microsoft SCCM

To import SCCM data into the CMDB, you can use the Service Graph connector for Microsoft SCCM instead of using the legacy SCCM connector.

Using the Service Graph SCCM connector provides these advantages:

- Adherence to the Common Service Data Model (CSDM) data model.
- Use of Identification and Reconciliation engine (IRE) to avoid duplicate records.
- Support for removed software detection and delta detection.
- Use of the IntegrationHub ETL which allows for easy data mapping and customizations.
- Higher performance during data processing.

For information on how to update from using the Microsoft SCCM connector plugin to using the Service Graph connector for Microsoft SCCM, see Update Microsoft SCCM 2016 plugin for Service Graph connector for Microsoft SCCM

Available modules

- **Setup:**
  - Configure the data sources.
  - Specify database server settings and the MID Server.
  - Test the configuration.

- **Scheduled Import**: Schedule the import or execute the import immediately.
- **Data Sources**: A list of the pre-configured data sources defining the external CMDB database.
- **Progress**: The progress log for scheduled imports.
- **Transform History**: A log of transformations performed by scheduled imports.
- **CI Identification**: Identifiers used by SCCM to match import set data with the CMDB.
- **Import Set Data**: Tables that store imported SCCM data.
- **Web Services**: List of web services used to add or remove fields in the transform maps.
Asset intelligence

Asset Intelligence is an SCCM feature that can filter, normalize and clean up software records. When enabled, it populates normalized software data in a separate table within the SCCM database. You can target this separate table instead of the raw software data table. When you import software records into the CMDB with this feature enabled, you get a cleaner set of software data. To use this feature, you must Activate SCCM Asset Intelligence scheduled imports in the target ServiceNow instance, as well as in the source SCCM database.

Activate a supported Microsoft SCCM plugin

The SCCM plugins can be activated by an administrator and requires the Integration - JDBC and CI Identification plugins. These dependent plugins are activated automatically with SCCM activation.

For a complete listing of the plugins that need to be activated, see Activate SCCM Asset Intelligence scheduled imports.

1. Navigate to System Applications > All Available Applications > All.
2. Find the plugin using the filter criteria and search bar.
   
   You can search for the plugin by its name or ID. If you cannot find a plugin, you might have to request it from ServiceNow personnel. For more information, see Request a plugin.
3. Click Install, and then in the Activate Plugin dialog box, click Activate.

   **Note:** When domain separation and delegated admin are enabled in an instance, the administrative user must be in the global domain. Otherwise, the following error appears: Application installation is unavailable because another operation is running: Plugin Activation for <plugin name>.

SCCM data import process and source tables

The Microsoft SCCM versions supported in the ServiceNow® platform offer identical features and the same imported data.

Data import process

1. A schedule called SCCM System <version> Import determines when the SCCM tables are imported into the ServiceNow® instance. Imports can be executed immediately or scheduled to run at defined intervals.
2. A MID Server retrieves the SCCM data and imports it into staging tables on the instance.
3. Transforms run on the data in the staging tables and map the SCCM data to existing fields in the CMDB.
**SCCM data imported**

This table shows the SCCM source tables, the corresponding import set staging tables in the ServiceNow® instance, and the target tables in the CMDB.
The ServiceNow® SCCM integration uses JDBC data sources to import software data from the SCCM database. Each data source contains the connection specifics for the SCCM database and names the MID Server the instance will use to import the data. The transforms that map the SCCM fields to the CMDB are defined in a related list in each data source record.

### Transform maps

Transform maps are accessed from the Transforms related list in each data source record. The source fields in SCCM and the target fields in the CMDB are listed in the Field Maps related list in each Table Transform Map record. The SCCM integration uses the transform map utility provided with the ServiceNow® platform. For instructions on editing or creating a transform map, see Transform maps.

The SCCM integration provides two transform maps for incremental software imports. Only one transform map can be enabled (Active) at a time.

- **Incremental Import**: Enabled by default. This map should be configured as Active when ServiceNow® Software Asset Management is not enabled on the instance.

*For more information about Software Asset Management and how to enable it, see Request Software Asset Management.*

### SCCM data sources

The ServiceNow® SCCM integration uses JDBC data sources to import software data from the SCCM database. Each data source contains the connection specifics for the SCCM database and names the MID Server the instance will use to import the data. The transforms that map the SCCM fields to the CMDB are defined in a related list in each data source record.

### Transform maps

Transform maps are accessed from the Transforms related list in each data source record. The source fields in SCCM and the target fields in the CMDB are listed in the Field Maps related list in each Table Transform Map record. The SCCM integration uses the transform map utility provided with the ServiceNow® platform. For instructions on editing or creating a transform map, see Transform maps.

The SCCM integration provides two transform maps for incremental software imports. Only one transform map can be enabled (Active) at a time.

- **Incremental Import**: Enabled by default. This map should be configured as Active when ServiceNow® Software Asset Management is not enabled on the instance.

*For more information about Software Asset Management and how to enable it, see Request Software Asset Management.*
• **Incremental Import (SAM enabled):** If the Software Asset Management plugin is activated, set this transform to *Active*

**Note:** To force a one-time full import of all software data from the SCCM database, clear the value in the "Last run datetime" field on the data source. This operation can take a long time to execute, so the most efficient method is to use an incremental transform after the first full import.

### Transforming the assigned user

The SCCM <version> Computer Identity transform script attempts to set the **Assigned to** field in the CMDB record by looking up the name of the user in the SCCM source table and comparing the value with the matching field in the ServiceNow sys_user table. If a match is found, that user is assigned to the record. If no match is found, the **Assigned to** field is left blank. The matching field is controlled by the `glide.discovery.assigned_user_match_field` system property, which is set to *user_name* by default.

### Identifiers

The SCCM integration uses CI identification to update CIs created from data imported from SCCM with a resource ID. The Hardware Rule identifier returns the resource ID of a computer from SCCM and stores it in the Source [sys_object_source] table. When resource IDs are first imported, either from SCCM or Discovery, the [sys_object_source] table is populated with IDs for each CI it identifies. In subsequent imports, if an incoming ID matches that of an existing CI, IRE (Identification and Reconciliation Engine) updates the information for that CI in the CMDB. If the incoming resource ID does not match that of an existing CI, IRE creates a new CI and populates it with the resource ID.

For more information about CMDB Identification and Reconciliation and IRE, see [CMDB Identification and Reconciliation](#).

Upgrades from pre-Geneva versions still preserve the legacy identifiers, but you can switch to the new identifiers using a property: `glide.discovery.use_cmdb_identifiers`. If you upgraded from a pre-Geneva version, you must manually add this property and set it to *true* to use the new identifiers. If you upgraded from Geneva, this property is available in the System Properties [sys_properties] table. To preserve functionality in custom legacy identifiers, convert them to the new CMDB identifier rules format before enabling this property. The system does not reconfigure your custom identifiers to the new framework automatically.

### Scripts

Data population scripts populate the related data in the CMDB for each target CI discovered by the Hardware Rule identifier.

### Software

The Microsoft SCCM integration reconciles the software package count in the records for a CI and removes a software instance from the Software Instance [cmdb_software_instance] table if the software package is uninstalled from the CI. For a full software import, the transform populates the Software [cmdb_ci_spkg] and Software Instance [cmdb_software_instance] tables. If the Software Asset Management plugin is enabled, the transform populates the Software Installation [cmdb_sam_sw_install] table.
**CAUTION:** The table data imported from SCCM must contain complete data for the CI. The instance assumes that the import represents all relationships that exist and adjusts the CMDB accordingly. Partial data received from SCCM tables can cause the deletion of active relationships.

**Configure the SCCM integration and schedule an import**

Importing data from Microsoft SCCM requires a connection to the SCCM database via a JDBC data source and a schedule that tells the MID Server when to fetch the data.

You must have sufficient credentials to query the SQL Server that contains the SCCM database. Create a SQL Server account in order to connect to the SCCM database on the MID Server to use the data sources.

Connect to your SCCM SQL Server and configure the following:

1. Create a new login user name and password for SQL Server authentication.
2. Choose the SCCM database that ServiceNow data sources will connect to.
3. Assign the 'db_datareader' role membership to the new user.

Role required: admin

The system uses the details of the database connection you create in this procedure to configure the default SCCM data sources automatically.

**Note:** If you want to configure the JDBC data source to authenticate on your SQL Server database using the Windows MID Server service user, select the **Use integrated authentication** box on each of the existing data sources.

1. Navigate to **Integration - Microsoft SCCM <version> > Setup.**
2. Complete the required fields to configure connection to the SCCM SQL database. Make sure to include a valid MID Server that has access to the SQL database server.

### SCCM data import setup

3. Under Related Links, click **Test data source connections** to test the connection to the SCCM database.
4. If the data source connects to the SCCM database, navigate to **Integration - Microsoft SCCM > Scheduled Import**.

The Scheduled Data Import form appears for your version of the SCCM integration. The Computer Identity data source runs first. The other data sources listed on the form run in sequence, based on their default order.
5. Select a calendar interval (Day, Week, etc.) in the **Run** field and specify the time of day the import should run. Your selection displays additional fields required to complete the schedule.

6. Click **Update** to schedule the import or click **Execute Now** to perform the import immediately.

   After the instance imports data using the **SCCM <version> Computer Identity** data source, the other data sources run in the order configured to retrieve the remainder of the SCCM data.

**Activate SCCM Asset Intelligence scheduled imports**

To prevent duplicate software imports, activate either the Asset Intelligence (AI) or the non-AI scheduled import.

Role required: admin

Make sure to limit the software import frequency to be no greater than the frequency of the table cleanup that tracks deleted software in SCCM.

Asset Intelligence is supported in these SCCM plugins:

- Integration - Microsoft SCCM 2007
- Integration - Microsoft SCCM 2012 v2
- Integration - Microsoft SCCM 2016

**Important:** To improve the performance of your initial SCCM import, you can prevent the system from checking against deleted software prior to the import date. Navigate to **Integration - Microsoft SCCM <version> > Data Sources > SCCM <version> Removed Software** and enter the current date in the **Last run datetime** field, using the format `yyyy-mm-dd 00:00:00.0`. This field is populated automatically for each subsequent run of the removed software data source, so it is not necessary to alter the value after the initial import.

1. Navigate to the **System Import Sets > Administration > Scheduled Imports**.
2. Set **Active** to **false** for these data import schedules:
   - SCCM <version> Software
   - SCCM <version> Removed Software
3. Set **Active** to **true** for these data import schedules:
   - SCCM <version> Software (with AI)
   - SCCM <version> Removed Software (with AI)

**Upgrade the SCCM integration version**

If you are using an earlier version of an System Center Configuration Manager(SCCM) plugin, you can switch over to a later version to take advantage of new features.

Role required: admin

The ServiceNow SCCM integrations are self-contained and can exist independently. They each use their own import set tables, data sources and transform maps. However, all SCCM integrations will transform data into the same tables within the ServiceNow CMDB. To avoid the data being overwritten by another source:

- Use one SCCM integration and disable all other SCCM scheduled imports.
- Perform a **full import** to clear the cmdb_software_instance table, the cmdb_sam_sw_install table, and other tables of old SCCM data.

**Note:** It is possible to configure each plugin to integrate with SCCM 2007 or 2012 because the mechanism of the integration is actually the same, which is to leverage Java Database Connectivity (JDBC) imports.
However, a data source must be modified if it is used for an SCCM version for which it was not written. Use the plugin version that corresponds to the SCCM version for which the data source is intended.

To change the SCCM integration:

- Disable the current integration by deactivating the SCCM import schedule.
- Activate the new SCCM plugin.
- Reimport all the software records when you are switching to an integration that supports incremental imports of removed software.

To disable the SCCM import schedule:

1. Navigate to Integration - Microsoft SCCM 20xx > Scheduled Import.
2. Clear the **Active** check box.

   ![Scheduled Data Import Form](image)

   **Scheduled Import form**

3. Click **Save** or **Update**.
4. To activate the new SCCM plugin, navigate to **System Definition > Plugins**.
5. Search on the name *SCCM* to see all the available SCCM integrations plugins.
6. Activate the plugin.
Migrate the Verizon eBonding Integration to a Production System

This topic outlines the tasks required for moving the Verizon eBonding integration from a Dev/Test environment to a Production environment.

This process requires coordination with your assigned Verizon implementation manager.

General Tasks

The following work can be performed any time:

- Obtain a production SOAP password from Verizon. Your Verizon SOAP user ID is the same as that used against the Verizon test broker.
- Create an integration user for Verizon in the ServiceNow Production instance. Use the same user name and password that was created for the development instance, so that the communication between Verizon and ServiceNow is properly authenticated.

Migrating to a Production Environment

Perform these tasks in order.

- Task 1: Request the Verizon eBonding plugin for the production instance. When the plugin is installed, the only immediate user interface change is an additional **Category** field named **VZ eBonding**. All of the triggers for the integration are dependent on the category being set to **VZ eBonding**. Enabling the plugin on the production instance should not affect your users. If you wish to take additional precautions, disable the **VZ eBonding** category from the list when the plugin is activated for the instance.
- Task 2: Set up the Verizon certificate and keystore. Copy these directly over from the Dev instance or regenerate them so that you have separate versions for the Dev and Production instances.
- Task 3: Configure the integration properties to work with the Production Verizon eBonding system. This is userID, password, and other properties provided by your Verizon representative.
- Task 4: Change all the Verizon eBroker SOAP Message functions to use Verizon’s production SOAP Endpoint. In most cases, the endpoint URL will be: https://pubwebsvc.vzbi.com:443/Trouble_Management_v3r0. Verify this URL with the Verizon implementation specialist.
  - In the **SOAP Message Functions** related list, click each function, clear the **Lock** check box, and enter the production endpoint.
  - Configure the **SOAP Message Functions** related list and add the **SOAP endpoint** column. In the **SOAP Message Functions** list view, unlock and update the endpoint for all records by editing multiple records.
- Task 5: Apply any customizations. If customizations to the integration on the Dev system were captured in an update set, apply that update set to the Production system.
- Task 6: Provide Verizon with the production SOAP Endpoint. The SOAP endpoint should look something like this: https://yourproductioninstance.service-now.com/ETMSPublish.do?WSDL.
- Task 7: Coordinate a Production turn up with your Verizon representative to do basic testing.

**Warning:** Do not create test tickets against the production system without working with the Verizon team. Any tickets created are treated as real tickets.

Legacy: Altiris integration 2.0

The Altiris integration is deprecated in the Istanbul release.

The Altiris integration a one direction import of the Altiris data into ServiceNow CMDB (Configuration management database). The integration keeps the ServiceNow CMDB up to date with Altiris SQLServer database.
**Data Import**

Relevant data is imported from the Altiris database to the CMDB. The Altiris database is not written to, it is considered an authoritative source. The import is achieved using a JDBC connection via the MID Server.

Information pulled from Altiris includes:

- PC Hardware (Model, Manufacturer, memory, clock speed, number of CPUs, etc.)
- Operating System Information (Name, Service Pack)
- Printers
- Disk information (physical, network, and logical)
• Network (IP Address, Netmask)

**Configuration and Operational Modules**

Enabling this integration will create the Integration - Altiris application. The following are the configuration and operational modules for this integration.

**Setup**

- Configure the data sources from one form
  - Provide the Database Server IP Address
  - Provide the Database Name
  - Provide the Database User ID and Password (this will need to be created on SQL DB side, see this article for help with this step: [http://technet.microsoft.com/en-us/library/aa337562.aspx](http://technet.microsoft.com/en-us/library/aa337562.aspx))
  - Find and select the MID Server
- Specify Database server settings and MID server
- Test configuration

**Scheduled Import**

- Schedule the execution of the import or import immediately

**Data Sources**

- A list of the pre-configured data sources defining the external CMDB database

**Progress**

- A historical list of progress on scheduled imports

**Transform History**

- A historical list of transformations performed during scheduled imports

---

**Warning:** If you have activated an existing integration of the previous version:

1. Activating the 2.0 plugin does not "add to" or "remove" anything from the existing integration.
2. If transitioning from the old integration to this new one, considerations need to be given to customizations already done eg. mapping enhancements or using different coalesce values, these will have to be re-implemented.
3. Both plugins could run at the same time, provided data is coalescing the same way - until there is no need for the older plugin at which time it can be turned off.

---

**Supported Versions**

The Altiris integration only supports Altiris version 6.5. The integration does not currently Altiris version 7.0.
Legacy Import set data for Altiris
This topic lists module names displayed by the Altiris import set data.

The Altiris import set data section shows a list of Import sets tables used in containing data retrieved from using JDBC to query the Altiris database. The module names (hence the import set tables they point to) match Altiris's table names and structure that it is loading from.

Module names

<i>Note:</i> Functionality described here requires the Integration - Altiris 2.0 plugin.

- Scheduled Cleanup
  - Configure a schedule to cleanup/delete import set data that have already been transformed
  - vComputer
  - Inv_AeX_OS_Operating_System
  - Inv_AeX_HW_CPU
  - Inv_AeX_HW_Memory
  - Inv_AeX_HW_Serial_Number
  - Inv_AeX_HW_Logical_Disk
  - Inv_AeX_OS_Add_Remove_Programs
  - Inv_AeX_AC_TCPIP

When viewing each of these table lists, at the end of the list you have links to other operational functions of the import set.

Related Links

Import Sets
Transform Maps
Transform History
Edit Web Service

Altiris integration application

- Import Sets
- Transform Maps
- **Transform History** - Log of completed import operations (where an import set was transformed into a table).
- Edit Web Service
Legacy: Web services import set tables for Altiris
This topic will list the modules that define the web service import set tables - the schema for the import set tables that are receiving the JDBC import.

From each web service, you can add/remove fields as well as access the transform maps to make modifications.

Note: Functionality described here requires the Integration - Altiris 2.0 plugin.

Related Links
Import Sets
Input Rows
Transform History

Import set tables
Import set tables

**Supported integration interfaces**

ServiceNow provides a number of interfaces to be able to directly integrate with the platform. These interfaces are considered part of the platform and are provided at no additional charge.

**Supported Integration Interfaces**

<table>
<thead>
<tr>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
</tr>
<tr>
<td>JDBC</td>
</tr>
<tr>
<td>JSON</td>
</tr>
<tr>
<td>LDAP</td>
</tr>
<tr>
<td>SOAP</td>
</tr>
<tr>
<td>REST API</td>
</tr>
<tr>
<td>SSO - SAML 2.0</td>
</tr>
<tr>
<td>Digest token authentication</td>
</tr>
<tr>
<td>ODBC</td>
</tr>
<tr>
<td>Data Export</td>
</tr>
<tr>
<td>CTI</td>
</tr>
<tr>
<td>Syslog probe</td>
</tr>
</tbody>
</table>

**Computer Telephony Integration**

Computer Telephony Integration (CTI) is accomplished by the CTI client on the user machine sending a URL to the instance.

The URL must have the following components:
1. The base URL. For example: https://<instance name>.service-now.com/cti.do? would get to the instance and ask for CTI processing.

2. Parameters identify what parts of the incident form to display.
   - **sysparm_caller_name**=name where 'name' is the name for a user.
   - **sysparm_caller_phone**=phone where 'phone' is the user's phone number. Either a name or phone should be provided if you want to identify the user on the call. Other parameters may be supplied to identify the user as discussed later.
   - **sysparm_task_id**=taskID where 'taskID' identifies an existing issue that the caller is calling about.
   - **sysparm_view**=view where 'view' is the name of the view to be used to display the data.
   - **sysparm_xxxx**=value where 'xxxx' is the name of a field within the 'incident' record that should be populated with the specified 'value'. For example sysparm_priority=1 would result in the priority field set to value of 1 when the new incident screen is shown.
   - **sysparm_cti_rule**=name where 'name' is the name of a function to be invoked for CTI processing rather than using the default script. The function must be defined in a sys_script entry marked client callable. If the function needs to insert, update, or delete any GlideRecord(s), it must call a separate non-client callable function to perform the update(s).

   **Note:** While the CTI Processing script has been changed to be client callable, the code implementing the task view has been commented out. You must implement a new non-client-callable function for the code that performs the task.update().

   **Note:** To make a script client-callable you must check the client-callable checkbox on the form that displays when the sys_script entry is displayed. The client-callable checkbox might not show by default. To show the client-callable checkbox, you may need to modify the fields that show on the form using the gear icon and slushbucket mechanism.

Parameters on the URL are available to the business rule as global values. For example:

```javascript
var name = sysparm_caller_name;
```

The business rule you specify must return the URL for the pop-up screen, and set the 'answer' global variable.

An example URL to bring up a screen shot for user Don Goodliffe would look like the following. https://<instance name>.service-now.com/cti.do?sysparm_caller_name=Don%20Goodliffe

Multiple sysparm parameters can be used, separated by ampersands (&).

**CTI Processing script**

When the **sysparm_cti_rule** parameter is not specified, the system uses the CTI Processing script to provide the following functionality.

The CTI Processing script does the following:

1. Tries to identify the user by the **sysparm_caller_name** value if it was supplied.
2. If no user has been found, the script tries to identify the user by the **sysparm_caller_phone** value if it was supplied.
3. If a user has been identified then one of the following is done
   a. If the user has open incidents, the popup screen shows information about the current caller and all the user's open incidents.
   b. If the user does not have any open incidents, the popup screen shows a new incident with information provided in the URL shown.
4. If a user was not identified and a taskID is given and the taskID exists, then nothing happens. The code to handle this case is commented out. If you want the popup screen to show the details for the task, you must modify the CTI Processing script to put the functionality in a separate non-client-callable function.

Integrating ServiceNow with your Intranet

You can add a ServiceNow login link to your intranet.

To deliver ServiceNow content from a web page, see Service Portal.

JDBCProbe

A JDBC probe runs on the MID Server to query an external database via [JDBC] and returns results to ServiceNow.

Probes interact with the MID Server via the ECC Queue, therefore the response of a JDBC probe returns as an XML payload in an "input" ECC Queue record. By default, each response payload will contain up to 200 returned rows, this value can be modified by setting the probe parameter `jdbcprobe_result_set_rows` to the desired number.

Activating the Plugin

Contact Customer Service and Support to activate the Integration - JDBC (com.snc.integration.jdbc) plugin.

1. Navigate to System Definition > Plugins.
2. Right-click the plugin name on the list and select Activate/Upgrade.

   If the plugin depends on other plugins, these plugins and their activation status are listed.
3. [Optional] Select the Load demo data check box.
   Some plugins include demo data—sample records that are designed to illustrate plugin features for common use cases. Loading demo data is a good policy when first activating the plugin on a development or test instance.
   You can load demo data after the plugin is activated by repeating this process and selecting the check box.
4. Click Activate.

Direct JDBC Probe

A direct JDBC probe specifies all the parameters necessary in the outbound ECC Queue XML payload.

It is a standalone probe that is decoupled from a JDBC Data Source and does not insert into an import set. The required field in the ECC Queue record for a direct JDBC probe is Topic and it must equal JDBCProbe. The Source field is reserved for the sys_id of the data source record in the case of a JDBC data source.

Note: If you have ServiceNow Discovery enabled on your platform, add the skip_sensor parameter to the probe to avoid the discovery sensors from processing the probe and resulting in a "No sensors defined" error.

XML Structure

A direct JDBC probe has the following XML payload structure

```xml
<parameters>
  <parameter name = "skip_sensor" value = "true" />
  <parameter name = "parameter_name" value = "parameter_value" />
...
  <parameter name = "work" >
    <select ... >
      ...
    </select>
  </parameter>
</parameters>
```

JDBC Probes via Data Source

JDBC probes are executed via a JDBC data source when an import is running against the data source.
A JDBC data source JDBC probe is described by the JDBCProbe Topic and the `sys_id` of the data source in the Source field of the ECC Queue output record.

The data source record would look like this

![Data Source](image)

**JDBC Data Source**

The following ECC Queue output probe will be created when you `load` from the data source.
JDBC Data Source Probe

Select * JDBC Probe short cut
Alternatively, you may specify a table_name parameter instead of a work element and the following query could be executed.

```
select * from <table_name>
```

For example, using the following XML payload

```
<?xml version= "1.0" encoding= "UTF-8" ?><parameters><parameter name = "jdbc_driver" value = "com.microsoft.sqlserver.jdbc.SQLServerDriver" />
<parameter name = "connection_string" value = "jdbc:sqlserver://xxx.service-now.com;databaseName=SMS_CRICKET;user=sms;password=sms" />
<parameter name = "table_name" value = "System_DATA" /></parameters>
```

Counting Rows

To count the number of rows in a table, you can indicate a select count(*) type query by including the count_rows parameter with a value of true.

For example

```
<?xml version= "1.0" encoding= "UTF-8" ?><parameters><parameter name = "jdbc_driver" value = "com.microsoft.sqlserver.jdbc.SQLServerDriver" />
<parameter name = "connection_string" value = "jdbc:sqlserver://xxx.service-now.com;databaseName=SMS;user=sms;password=sms" />
<parameter name = "count_rows" value = "true" /><parameter name = "table_name" value = "System_DATA" /></parameters>
```

The resulting response XML payload

```
<parameters>
...  
<result query = "SELECT count(*) as row_count FROM System_DATA" ><row id = "1" ><row_count class = "java.lang.Integer" length = "11" type = "4" >2312</row_count></row></result>
```
Parameters
The following parameters are available in a direct JDBC probe.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jdbc_driver</td>
<td>Required. Java class name for the JDBC driver to use, the currently supported drivers are:</td>
</tr>
<tr>
<td></td>
<td>• Oracle: oracle.jdbc.OracleDriver</td>
</tr>
<tr>
<td></td>
<td>• Microsoft SQL Server: com.microsoft.sqlserver.jdbc.SQLServerDriver</td>
</tr>
<tr>
<td></td>
<td>• MySQL: com.mysql.jdbc.Driver</td>
</tr>
</tbody>
</table>

Example

com.microsoft.sqlserver.jdbc.SQLServerDriver

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>connection_string</td>
<td>Required. JDBC connection string/URL for defining the connection, usually contains information about the database server and name, the user ID and password for connection to the database. The syntax is vendor specific, refer to the following links for reference:</td>
</tr>
<tr>
<td></td>
<td>• Oracle: [jdbc:oracle:thin:&lt;username/password&gt;@&lt;database&gt;]</td>
</tr>
<tr>
<td></td>
<td>• Microsoft SQL Server: [jdbc:sqlserver://localhost;user=MyUserName;password=*****;]</td>
</tr>
<tr>
<td></td>
<td>• MySQL - [jdbc:mysql://localhost/database?user=username%26password=passwd]</td>
</tr>
</tbody>
</table>

Example

jdbc:sqlserver://xxx.service-now.com;
databaseName=SMS;
user=sms_user;
password=sms_password;

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>work</td>
<td>Required if not using the table_name parameter short cut.</td>
</tr>
<tr>
<td></td>
<td>Parent element of an XML fragment describing the SQL command to execute.</td>
</tr>
</tbody>
</table>

Example

...
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>query_timeout</td>
<td>Optional during SELECT. Number of seconds the JDBC driver will wait for a query (SELECT) to complete. Zero means no timeout. If timeout is exceeded, the integration considers the JDBC result inaccessible and places it in an error state.</td>
</tr>
<tr>
<td>table_name</td>
<td>Optional (except required during count_rows == true). Alternate way of executing a select * query; instead of using the work element. Equivalent to executing select * from &lt;table_name&gt;.</td>
</tr>
<tr>
<td>count_rows</td>
<td>Optional. Indicates whether a select count(*) query should return the number of rows (true/false). The result of the count will be returned as a row_count element in the result element.</td>
</tr>
<tr>
<td>query</td>
<td>Optional. Type of query. Possible choices are &quot;All Rows from Table&quot; or &quot;Specific SQL&quot;. If &quot;Specific SQL&quot;, the sql_statement will be required to specify the SQL statement.</td>
</tr>
<tr>
<td>sql_statement</td>
<td>Optional. Use a specific SQL query. The presence of this element executes a direct query specified in the value attribute.</td>
</tr>
<tr>
<td>skip_sensor</td>
<td>Optional. Determines if Discovery will attempt to process the ECC input from the JDBCProbe. Default = true</td>
</tr>
</tbody>
</table>
For example, to query a table using a direct JDBC probe, requires the following parameters:

- JDBC driver class name
- JDBC connection string
  - Database server
  - Database name
  - User name
  - User password
- The table name

```xml
<?xml version="1.0" encoding="UTF-8"?>
<parameters>
    <parameter name="jdbc_driver" value="com.microsoft.sqlserver.jdbc.SQLServerDriver"/>
    <parameter name="connection_string" value="jdbc:sqlserver://xxx.service-now.com;databaseName=SYS;user=sms_user;password=sms_password"/>
    <parameter name="work">
        <select table="System_DATA"/>
    </parameter>
</parameters>
```

Queue form

**Using the Work Element**

The work element encodes SQL statements to be executed by the probe.

The following are the valid **work** child elements.

- select
- update
- insert
- delete
**SELECT**

Retrieve rows from the specified table in the database specified by the JDBC connection string. The simplest `select` work just specifies the table name and will retrieve all fields in a row, for example:

```xml
...<parameter name= "work" ><select table = "System_DATA" /></parameter>...
```

To specify a search criteria, specify the `where` attribute on the `select` element, for example:

```xml
...<parameter name= "work" ><select table = "System_DATA" where = "InstanceKey=692" /></parameter>...
```

To specify the fields you want returned, embed the fields as child elements of the `select` element, for example:

```xml
...<parameter name= "work" ><select table = "System_DATA" where = "InstanceKey=692" ><MachineID /><SMSID0 /></select></parameter>...
```

To use a direct SQL statement, specify it in the `query` parameter

```xml
...<parameter name= "query" value= "Specific SQL" /><parameter name = "sql_statement" value = "select * from any_table where value='test'" />
...```

**UPDATE**

An `update` SQL can be executed by specifying the `table`, optional `where` clause and required child elements for the fields and their values to update.

```xml
...<parameter name= "work" ><update table = "alerts.status" where = "ServerName = 'NCOMS' AND ServerSerial=3935" ><Agent>ServiceNow - INC10020</Agent><URL>http://Macintosh-9.local:8080/glide/incident.do?sys_id=17a31f380a0abaee048ca875e8891d0</URL><Severity quoted = "false" >3</Severity><Acknowledged quoted = "false" >0</Acknowledged></update></parameter>...
```

**INSERT**

An `insert` SQL can be executed by specifying the `table`, and required child elements for the fields and their values to insert.

```xml
...<parameter name= "work" ><insert table = "alerts.status" ><Agent>ServiceNow - INC10020</Agent><URL>http://Macintosh-9.local:8080/glide/incident.do?sys_id=17a31f380a0abaee048ca875e8891d0</URL><Severity quoted = "false" >3</Severity><Acknowledged quoted = "false" >0</Acknowledged></insert></parameter>
```
DELETE

A delete SQL can be executed by specifying the table, and optional where clause.

```xml
<parameter name= "work" ><delete table = "alerts.status" where = "ServerName \%= 'NCOMS' AND ServerSerial=3935" /></parameter>
```

Build a search provider for your instance

ServiceNow Search Providers allow you search and our Forums from the IE and Firefox search bar.

In Firefox 3.x you can also assign a keyword to each Search Provider and access them from the address bar.
For example, assign w to the wiki search provider and you can search the wiki for Business Rules by typing: w business rules in the address bar.

```
<?xml version="1.0" encoding="UTF-8"?>
<OpenSearchDescription xmlns="http://a9.com/-/spec/opensearch/1.1/">
  <ShortName>Demo Search</ShortName>
  <Description>Demo Search provider</Description>
  <InputEncoding>UTF-8</InputEncoding>
  <Url type="text/html" template="https://www.service-now.com/demo/nav_to.do?
      uri=incident_list.do?sysparm_query=active%3Dtrue^123TEXTQUERY321%3D{searchTerms}"/>
</OpenSearchDescription>
```

Search Bar

1. Create an opensearch description document. You can review the OpenSearch standards for details on additional attributes of this document such as including an icon.

```
<?xml version="1.0" encoding="UTF-8"?>
<OpenSearchDescription xmlns="http://a9.com/-/spec/opensearch/1.1/">
  <ShortName>Demo Search</ShortName>
  <Description>Demo Search provider</Description>
  <InputEncoding>UTF-8</InputEncoding>
  <Url type="text/html" template="https://www.service-now.com/demo/nav_to.do?
      uri=incident_list.do?sysparm_query=active%3Dtrue^123TEXTQUERY321%3D{searchTerms}"/>
</OpenSearchDescription>
```

2. Save the file to a web server with xml extension. The method used to install doesn't allow local file calls.
3. Create a simple html page to install the provider.

```
<a href="javascript:window.external.AddSearchProvider('http://yourServer/
      yourFile.xml');">
```
You could try running the JavaScript command from the browser location box instead of using the html file. This works with FF not IE.

**Syslog probe**

The ServiceNow Syslog probe uses the MID Server to deliver log messages from a ServiceNow instance to another machine, such as a dedicated log server, using the syslog protocol over an IP network.

**How the Syslog probe works**

The syslog probe is launched by a ServiceNow Script Include (called Syslog) that can be invoked from a business rule, event, or Orchestration activity and is launched by a MID Server. A syslog server or any server that can receive messages using the syslog protocol must be installed on the recipient (target) machine. Typically, a dedicated log server in the network is configured to receive all internal syslog messages. Some products that accept syslog messages are:

- ArcSight
- Splunk
- LogLogic
- syslog-ng

**Example**

The Acme Corporation wants to send a log message from their ServiceNow instance to an ArcSight syslog server inside their corporate firewall each time a user login fails. The system administrator uses the login.failed event to trigger a business rule that invokes the Syslog Script Include each time a login fails. Acme’s MID Server checks the ECC Queue for work and picks up the syslog probe, which contains the log entry. The MID Server then sends the log message to the ArcSight server, which gathers log messages from all the machine in the internal network.
The following code sample, included in an event or a business rule, directly calls the Syslog Script Include and sends a syslog message to a designated syslog server:

```javascript
var sl = new Syslog('FQDN of your syslog server', 'mid.server.Eclipse', 16);
sl.log('This is a sample log message', 6);
```

This code does the following:

- Sends the log message to facility 16
- Sets the priority to 6 (informational)
• Sends the message to your syslog server
• Launches the probe via the MID Server named "Eclipse"

Domain separation in third-party application and data source integration

This is an overview of domain separation and integration of third-party applications and data sources. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can control several aspects of this separation, including which users can see and access data.

Support level: Basic-Standard

The Basic-Standard level of domain separation is achieved through data visibility as well the integration design.

Basic
• There is business logic to ensure data goes into the proper domain for the application’s service provider use cases.
• In the application, the user interface, cache keys, reporting, rollups, aggregations, and so on, all consider domain at run time.
• The owner of the instance needs to be able to set up the application to function normally across multiple tenants.

Standard
• Includes Basic level
• Business logic: Processes can be created or modified per customer by the service provider. The use cases reflect proper use of the application by multiple service provider customers in a single instance.
• The owner of the instance needs to be able to configure MVP business logic and data parameters per tenant as expected for the specific application.

Overview

Team should define a few examples with data-driven properties. There should be three different buckets with short description for each one

User administration

Manage the individuals who can access your instance by defining them as users in the system. Create user groups, and assign users to them. Use roles to specify what different users and user groups can see and do.

A group is a set of users who share a common purpose. Members of groups perform tasks such as approving change requests, resolving incidents, receiving email notifications, or performing change request tasks. Assign every user to at least one group.

A good practice is to assign roles to groups rather than to users. Administrators can assign roles quickly to multiple users by adding the users to the group. If a user moves to another group, the role assigned to the new group is applied automatically.

Manage user administration system properties

The administrator can add or modify system properties to let users view their profile, automatically create a user record from a registration request, and modify the impersonate option

© 2021 ServiceNow, Inc. All rights reserved.
Allow a user to view a profile

Users are able to view their profile by clicking their name in the Welcome banner. If your users cannot do this, enable a system property.

Role required: admin

2. Search for the `glide.ui.welcome.profile_link` property.
3. Set the value to `true`.

Enable auto processing of a request

You can enable auto processing of user self-registration requests by setting a property.

Role required: admin

When the `Enable auto processing of user registration requests` property is enabled, user accounts are automatically created upon registration.

1. Activate the User Registration Request (com.snc.user_registration) plugin. The User Registration Request plugin provides the ability for unregistered users to request access to a ServiceNow instance. For more information, see Activate a plugin.
2. Navigate to System Properties > System.
3. Select the check box for the property Enable auto processing of user registration requests.
4. Click Save.
   
   If enabled, registration requests do not require approval. Instead, the business rule Auto-Process User Registration creates the user record from the information provided.

Show or hide impersonation button

You can set a system property to show or hide the impersonation button. By default, the system shows the impersonation button.

Role required: admin

The system property only controls the visibility of the impersonation button, which is rendered by the `impersonate_button` UI macro. The impersonation button opens the `impersonate_dialog` UI page. Modifying either the impersonation UI macro or impersonation UI page are not recommended.

1. Navigate to System Properties > UI Properties.
2. Clear Enable impersonation button in banner line to hide the impersonation button, or select it to show the impersonation button.
3. Click Save.

Administrators can still access impersonation by navigating directly to the `impersonate_dialog` UI page.
Add a new company

You can add companies that represent vendors, manufacturers, or customers with whom you do business. These companies provide a way to categorize users, groups, and assets.

Role required: user_admin or admin

1. Navigate to User Administration > Companies.
2. Click New.
3. Complete the fields, as appropriate.

**Company fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the company.</td>
</tr>
<tr>
<td>Phone</td>
<td>Company phone number.</td>
</tr>
<tr>
<td>Fax phone</td>
<td>Company fax number.</td>
</tr>
<tr>
<td>Manufacturer</td>
<td>Whether the company is a manufacturer.</td>
</tr>
<tr>
<td>Vendor</td>
<td>Whether the company is a vendor.</td>
</tr>
<tr>
<td>Stock symbol</td>
<td>Three or four letter stock symbol for the company.</td>
</tr>
<tr>
<td>Stock price</td>
<td>Current price at which company stock is sold.</td>
</tr>
<tr>
<td>Street</td>
<td>Mailing street address of the company.</td>
</tr>
<tr>
<td>City</td>
<td>City in which the company is located.</td>
</tr>
<tr>
<td>State</td>
<td>State or province in which the company is located.</td>
</tr>
<tr>
<td>Zip/Postal code</td>
<td>Zip or postal code for the company.</td>
</tr>
<tr>
<td>Notes</td>
<td>Any information about the company that would be helpful for others to know.</td>
</tr>
</tbody>
</table>

Fields that can be added by configuring the form:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Latitude</td>
<td>The latitude of the company, if applicable. This field is populated by a business rule called <strong>get_lat_long</strong>. Deactivate this business rule to prevent the system from overwriting any values populated in the field manually. Latitude is expressed as a floating point data type. Latitude from upgraded versions of ServiceNow expressed in any format other than floating point appears in a column called <strong>Old Latitude</strong>. The system attempts to convert all latitude values from previous versions to the floating point notation, where possible.</td>
</tr>
</tbody>
</table>
### Longitude

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Longitude</td>
<td>The longitude of the company, if applicable. This field is populated by a business rule called get_lat_long. Deactivate this business rule to prevent the system from overwriting any values populated in the field manually. Longitude is expressed as a floating point data type. Longitude from upgraded versions of ServiceNow expressed in any format other than floating point appears in a column called Old Longitude. The system attempts to convert all longitude values from previous versions to the floating point notation, where possible.</td>
</tr>
</tbody>
</table>

**Note:** The IT Finance application adds a Finance view to the Company form. The Finance view adds a chart that shows expenses that were allocated to the company. For more information, see Finance Service Management.

### Add a department

Departments provide another way to categorize users, groups, and assets. You can add departments and assign them to users.

Role required: user_admin or admin

An administrator may need to configure the form to show all the fields listed in the steps.

1. Navigate to **User Administration > Departments** and create a new record.
2. Enter or modify the department name, ID, and description.
3. Optional: Select the company the department is associated with.
4. Optional: Add a department head, primary contact, or both from your list of users.
5. Optional: Add the parent department, if applicable.
6. Click **Submit**.

### Create a user

You can add a user to your instance to allow them to log in and use the features.

Role required: user_admin

1. Navigate to **User Administration > Users**.
2. Click **New** and enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Input Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>Create a unique identifier for this user’s ServiceNow login user name. Typical examples of user IDs are cwitherspoon and charlie.witherspoon. You cannot create a new user whose User ID duplicates an existing user. If you do import duplicates from an update set, the more recently created name takes the duplicate User ID.</td>
</tr>
<tr>
<td>First name</td>
<td>Enter the user's full first name.</td>
</tr>
<tr>
<td>Field</td>
<td>Input Value</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Last name</td>
<td>Enter the user's last name.</td>
</tr>
<tr>
<td><strong>Note:</strong> You can clear the First Name field, or the Last Name field in an existing user record, but you cannot clear both at the same time.</td>
<td></td>
</tr>
<tr>
<td>Title</td>
<td>Enter a title or job description, or select one from the list.</td>
</tr>
<tr>
<td>Department</td>
<td>Select the user's department from the list.</td>
</tr>
<tr>
<td>Password</td>
<td>Assign a password to the user. This password can be permanent or temporary.</td>
</tr>
<tr>
<td>Password needs reset</td>
<td>Select this check box to require the user to change the password during the first login.</td>
</tr>
<tr>
<td>Locked out</td>
<td>Select this check box to lock the user out of the instance and terminate all their active sessions. The system prevents users with the admin role from locking themselves out.</td>
</tr>
<tr>
<td>Active</td>
<td>Select this check box to make this user active. Only the administrator sees inactive user in:</td>
</tr>
<tr>
<td></td>
<td>• Lists of users</td>
</tr>
<tr>
<td></td>
<td>• The selection list on reference fields (magnifying glass icon)</td>
</tr>
<tr>
<td></td>
<td>• The auto-complete list that appears when you type into a reference field</td>
</tr>
<tr>
<td>Web service access only</td>
<td>Select this check box to designate this user as a non-interactive user. This field is available with Non-Interactive Sessions.</td>
</tr>
<tr>
<td>Internal Integration User</td>
<td>Select this check box to designate this user as an internal integration user.</td>
</tr>
<tr>
<td>Date format</td>
<td>Select the user's preferred format for dates.</td>
</tr>
<tr>
<td>Email</td>
<td>Enter the user's email address. To enter a non-standard email address that does not pass field validation, you must deactivate the validation script first.</td>
</tr>
<tr>
<td>a.</td>
<td>Navigate to System Definition &gt; Validation Scripts.</td>
</tr>
<tr>
<td>b.</td>
<td>Select the email record.</td>
</tr>
<tr>
<td>c.</td>
<td>Clear the Active check box and save the change.</td>
</tr>
<tr>
<td>d.</td>
<td>Complete the user profile, including the email address, and update or submit the record.</td>
</tr>
<tr>
<td>e.</td>
<td>Reactivate the email validation script.</td>
</tr>
<tr>
<td>Field</td>
<td>Input Value</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Notification</td>
<td>Specify if email notifications should be sent to this user. Select <strong>Enable</strong> if an email notification should be sent to this user. Select <strong>Disable</strong> if the user can still receive notifications if they subscribe to the notification, or are specified as a recipient in the Email Notifications form. To prevent notification completely, set a condition on the Email Notification form itself that does not deliver the notification if this field is set to <strong>Disable</strong>.</td>
</tr>
<tr>
<td>Calendar integration</td>
<td>Select <strong>Outlook</strong> to have this user receive meeting notifications via email directly to the calendar. Otherwise, select <strong>None</strong>.</td>
</tr>
<tr>
<td>Time zone</td>
<td>Select the user's time zone.</td>
</tr>
<tr>
<td>Business phone</td>
<td>Enter this user's business phone number.</td>
</tr>
<tr>
<td>Mobile phone</td>
<td>Enter this user's mobile phone number.</td>
</tr>
<tr>
<td>Photo</td>
<td>Attach a photo of the user, if appropriate.</td>
</tr>
<tr>
<td>Geolocation tracked</td>
<td>Select the check box to enable location tracking. The <strong>Geolocation tracked</strong> field, which is available when Geolocation is activated, provides the option to track a user's location.</td>
</tr>
<tr>
<td>Location</td>
<td>Select the user's usual location. This field is visible when geolocation is active.</td>
</tr>
</tbody>
</table>

3. Optional: Customize the form to add the **Schedule** field and assign a **schedule** to the user.

4. Optional: Customize the form to add a **Language** field or a **Country code** field to associate a specific language or location with a user.

5. Click **Submit**.
   The new user record appears at the top of the list.

### Deactivate the validation script during user creation

To enter a non-standard email address that does not pass field validation, you must deactivate the validation script first.

Role required: admin

1. Navigate to **System Definition > Validation Scripts**.
2. Select the **email** record.
3. Clear the **Active** check box and save the change.
4. Complete the user profile, including the email address, and update or submit the record.
5. Reactivate the email validation script.
User preferences

Individual users can configure many UI features, such as the number of rows per page in a list or whether the response time displays at the bottom of a v2 list or form.

These user customizations are stored as records in the User Preference [sys_user_preference] table, and are updated each time the user changes the setting.

The UI displays according to each user's preferences.

For example, by default the response time may appear at the bottom of v2 lists and forms. If a user hides the response time, a user preference record is created showing the response time indicator as hidden. During the user's future sessions, the response time indicator is hidden. If the same user later displays the response time, the user preference record is updated appropriately and future sessions open with the response time indicator visible.

Navigate to User Administration > User Preferences for a list of user preference records. Click a preference name to display that preference in form view.

Note: Having more than 10,000 user preferences causes system degradation and UI performance issues.

User Preferences form
### User preference fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the feature or functionality.</td>
</tr>
<tr>
<td>Description</td>
<td>An optional short description of the feature or functionality.</td>
</tr>
<tr>
<td>System</td>
<td>Shows whether this record indicates the system-wide default (TRUE), or not (FALSE).</td>
</tr>
<tr>
<td>Type</td>
<td>Shows the data type of entry accepted for the Value. For example, you can select string or integer.</td>
</tr>
<tr>
<td>User</td>
<td>Shows the name of the user for whom the setting is customized. If User is blank, the record is for a system-wide default.</td>
</tr>
<tr>
<td>Value</td>
<td>The current setting for this record. Compare this value to the User field and System field to determine whether the value shown is a system-wide default or a specific user’s preference.</td>
</tr>
</tbody>
</table>

Records for the system-wide value, which applies to users who have not customized the feature, have these values: **System=True** and **User=blank**. For each user who customizes the features, a separate record is created with these values: **System=False** and **User=<username>**. As a result, the same customizable UI feature may have multiple user preference records.

For some features, the system-wide record does not appear in the User Preferences module initially. The system-wide record may be added to the User Preferences list when a user record is created for the same feature.

When an administrator manually changes a user's preference value through this module, the user's next session uses the administrator's setting. However, the user can customize the features again through the UI, which updates their user preference record. If the administrator deletes the user preference record for a particular user, that user's next session uses the system-wide value for that feature. When the user later customizes the feature, the system creates a user preference record for the user.

### Global user preferences

Create global preferences to set a default preference for your users. To make a preference the default, create a preference, check the **System** check box, and leave the **User** field blank. The preceding image is an example of a global preference. This preference is applied to all users. This preference is overridden for a specific user by creating a preference with the same name that has a value in the **User** field.

**Note:** You should never have more than one preference with the same name set as a global user preference.

### User preferences and update sets

User preference records for system-wide values, also called the default or global values, are stored in update sets. Any changes are implemented when you import the update set and affect all users who have not customized the feature.

User preference records for specific users are not stored in update sets, so user customizations are retained when you import an update set.
Troubleshooting user-specific UI differences

If a user encounters an unexplained behavior in the user interface, an administrator can check their user preferences. Navigate to User Administration > User Preferences. Search for the user name to find all that user's records. Delete the record that affects the behavior in question.

The system-wide preference is active during the user’s next session. If the user customizes the behavior, a new user preference record is created and used for subsequent sessions.

User self-registration

The User Registration Request [com.snc.user_registration] plugin provides the ability for unregistered users to request access to a ServiceNow instance. An administrator can activate the plugin.

A user can request an account by navigating to the instance. If the plugin is installed, the following section is added to the welcome screen.

Request a user account

If you do not yet have a user account your can request one using the self registration form.

The user can complete and submit the self-registration form, and see a confirmation that it was submitted. The user receives an email when the account is registered.

Note: If the email address entered in the self-registration form is already in the system, the request is not submitted.

Approve an account

When a user submits a self-registration form, it can be reviewed and approved.

Role required: admin

1. Navigate to User Administration > Pending User Registrations and open the request.
2. Use the Create User and Reject related links on the registration request form to approve or deny the request.

   • If Create User is selected, a new user is created using the email address as the User ID.
   • If Reject is selected, the request is marked Rejected.

The user is sent an email notification with the login information if the request was accepted, or the rejection information.
3. Optional: To view past registration requests, remove the [State] [is] [Pending] condition from the filter in the list view.

Impersonate a user

Administrators can impersonate other authenticated users for testing purposes and view impersonation logs.

When impersonating another user, the administrator has access to exactly what that user can access in the system, including the same menus and modules. The instance records anything the administrator does while impersonating another user as having been done by that user.

Impersonation limitations

- When you impersonate any user, all scope-protected roles and encryption context roles are removed from the user being impersonated. However, if the impersonating user (the admin, for example) has a scope-protected role, that role is not removed from the list of roles for the user being impersonated.
- When you impersonate a user with an application-specific admin role (for example, an application admin for Human Resources or Security Incident Response), you cannot access features granted by the application admin role, including security incidents, profile information, or other scope-protected features, unless you already have those roles. Access to modules and applications in the navigation bar is also restricted. Admins cannot change the password of any user with an application admin role.
- The following actions or conditions cause a user impersonation to end:
  - The user impersonates a different user
  - The user session ends, for example after a user logs out of their instance

Note: The Impersonate Begin event appears in the system log (syslog.list) when impersonation begins, and the Impersonate End event appears in the system log when impersonation ends according to one of the two conditions listed above.
Impersonation requirements

The user account to be impersonated must have a user ID. You can find this ID in the User [sys_user] record for the account. If this value is missing, the message The user you selected could not be impersonated appears.

You need several different logins to test the system:

• An admin account to do work.
• An itil (or similar) login to test as a technician.
• An ess login to test as an end user.

More logins may be required to adequately test the system.

Note: When you attempt to impersonate a user who is locked out or is inactive, the system forces a logout after you generate an event or click a link. All changes made while using impersonation affect the current session. Make sure you properly logout, then login after impersonation is completed.

Mobile impersonation

Mobile impersonation is available on ServiceNow mobile apps. For information on mobile impersonations, see Mobile impersonation

Impersonate a user in UI16

You can select a user or enter a different user name to perform impersonation.

Role required: impersonator

1. In the banner frame, click your user name to open the user menu.
2. Select Impersonate User.
   The Impersonate User dialog box appears.
3. Select a user from the Recent Impersonations list or enter a different user’s name in the user selection field.
4. To return to your original login, follow these same steps then select your name from the list.

Impersonate a user in UI15

You can click the impersonate icon and select a user name to perform impersonation.

Role required: impersonator

1. Click the impersonate icon ( ) in the banner frame.
   The Impersonate User dialog box appears.
2. Select the user from the Recent Impersonations list, click the lookup icon and select the user's name from the full list, or type the user's name.
3. Click OK.

Impersonation logs

Impersonations are logged in the System Log.

Log impersonations for either interactive (UI) or non-interactive sessions.
Impersonation logging for interactive sessions

Interactive sessions are performed through the user interface (UI). Enable or disable impersonation logging for interactive sessions using the `glide.sys.log_impersonation` property.

If you enable impersonation logging for interactive sessions by setting `glide.sys.log_impersonation` to `true`, all interactive sessions are recorded in the impersonate log.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>glide.sys.log_impersonation</code></td>
<td>Enables (true) or disables (false) impersonation logging for interactive sessions.</td>
</tr>
</tbody>
</table>

Impersonation logging for non-interactive sessions

Non-interactive sessions are performed by applications and scripts, not through the UI.

Impersonation logging of non-interactive sessions is turned off by default. If you enable impersonation logging by setting the `glide.sys.log_impersonation.non_interactive` property to `true`, impersonations of non-interactive sessions are recorded in the impersonate log.

Even with `glide.sys.log_impersonation.non_interactive` set to `true`, the system does not log certain common impersonation tasks performed on behalf of the default users (`system`, `soap.guest`, and `guest`) because the application impersonates those default users to perform a variety of tasks.

Use the `glide.sys.log_impersonation.non_interactive.exclusion` property to exclude impersonations by other users in addition to the default users.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>glide.sys.log_impersonation.non_interactive</code></td>
<td>Enables (true) or disables (false) impersonation logging for non-interactive sessions.</td>
</tr>
<tr>
<td><code>glide.sys.log_impersonation.non_interactive.exclusion</code></td>
<td>Excludes impersonation logging of non-interactive sessions for specified users. Enter user names as a comma-separated list. Default users (<code>system</code>, <code>soap.guest</code>, and <code>guest</code>) do not need to be included in the list.</td>
</tr>
</tbody>
</table>

Force logout

In some cases, impersonating a user might cause an issue that makes it difficult to switch back (for example, if in a test environment, the user is being presented with a broken page).

To return to the user, navigate to `http://<instance name>.service-now.com/logout.do` and log back in.

Manage user sessions

The Now Platform provides the ability to view and terminate individual user sessions, lock out users from the system, and make users inactive.

- Terminating a specific user session effectively logs that user out of the next transaction, which is usually the next browser click. Use the terminate sessions feature when you want to perform system maintenance.
- Locking a user out of the system means the user can no longer log in or generate any actions from any email messages that the user sends to the instance. Locking out users also terminates their user sessions.
• Making a user inactive means that the user does not show up in any fields that reference active users on the User table.

Modify session timeout

The base system uses the default Apache session timeout of 30 minutes.

Role required: admin

After 30 minutes of inactivity in the application, the platform logs the user out automatically, unless the Remember Me check box in the login screen is selected. Making the interval longer can lead to the unnecessary maintenance of inactive sessions in memory. Adjust this timeout setting to no more than a few hours, although up to 24 hours is workable.

**Note:** Regardless of how many windows a user has open in a browser, it is considered to be one session. However, if a user has two separate browsers open (such as Internet Explorer and Firefox), it is considered to be two separate sessions.

1. Clear the Remember Me check box in the login screen.
2. In the Navigator pane, enter `sys_properties.list`.
3. In System Properties, search for `glide.ui.session_timeout`.
4. If `glide.ui.session_timeout` does not exist, click **New** to add a new property using the following values:
   * **Name**: glide.ui.session_timeout
   * **Description**: Type a brief description. In this case, enter something like Override the default session timeout (30). This value is in minutes.
   * **Type**: Select the appropriate data type. In this case, select **Integer**.
   * **Value**: Change the default value from 30 minutes to a value of your choice.

**Note:** The session timeout can also be set through installation exit customizations.

• Ajax calls to the server keep the session alive (such as Labels and Refreshing homepages).
• Polling keeps the session alive when the chat desktop is open (requires the Chat plugin).
• Administrators can add the following properties to the System Properties table.
  * `glide.security.csrf.handle.ajax.timeout`: Handles errors for timed out Ajax requests when set to `true`.
  * `glide.security.auto.resubmit.ajax`: Automatically resubmits timed-out Ajax requests when set to `true` and the Remember Me check box is selected or automatically set. A popup appears to users asking them to continue.
  * `glide.ui.auto_req.extend.session`: When set to `true`, the system automatically extends a user's session by the value the user selects for the homepage refresh time. If there is no homepage refresh time, the standard timeout value applies. Tablet and mobile devices do not support this property. When set to `false`, user sessions time out when the Remember me check box is clear. The timeout is based on whether there is a homepage refresh time. When there is no homepage refresh time, the standard timeout value applies. When there is a homepage refresh time, the user session times out after the timeout value plus one interval of the homepage refresh time. For example, if a user selects to refresh interval of five minutes, then user sessions expires after the timeout value plus five minutes.

**Note:** Users who select the Remember me check box are unaffected by session timeout properties.
• Administrators can also add the following properties to configure an alternate session timeout value for guest sessions. You can do this to conserve system resources:

  • **glide.session.unauthorized.timeout.enabled**: If set to **true**, enables an alternate session timeout for unauthenticated, guest sessions. Guest sessions are created for HTTP requests to the instance that do not contain authentication information. By default this property is set to true.

  • **glide.unauthorized.session_timeout**: The session timeout value in minutes that controls the lifespan of an unauthenticated (unauthenticated) guest session. Set the property to a value greater than 0 and less than the value in the **glide.ui.session_timeout** property.

**Lock out a user**

Lock out a user when you do not want the user to access the instance.

Role required: user_admin or admin

1. Navigate to **User Administration > Users** and select the user from the list.
2. Select the **Locked Out** check box, and update the record.

**Mark a user inactive**

You can mark a user inactive so the user does not show up in any fields that reference active users on the User table.

**Note:** By default, when you mark a user inactive, you lock out that user. The Lock Out Inactive Users business rule governs this behavior.

1. Navigate to **User Administration > Users** and select the user from the list.
2. Clear the **Active** check box, and update the record.

**Terminate a specific user session**

You can terminate a user session, for example, if you are going to perform system maintenance and users are still logged in.

1. Navigate to **User Administration > Logged in users**.
   You can only see users who are logged into the same application node as you. If the Active field on a user record value is false, the user is logged in but not currently running a transaction. Most users appear as inactive at any given time.
2. Select the session you want to end.
3. Click **Lock Out Session**.
   The session is terminated, and the user is redirected to the login page at the next attempted transaction. The user is not locked out. Multiple user sessions may be associated with one user. Terminating a user session only affects the specific session.

**Groups**

A group is a set of users who share a common purpose.

Groups may perform tasks such as approving change requests, resolving incidents, receiving email notifications, or performing work order tasks. Any business rules, assignment rules, system roles, or attributes that refer to the group apply to all group members automatically. Users with the user_admin role can create and edit groups.
Create a user group

Create groups and assign roles to them. Users assigned to the group inherit the roles.

Role required: user_admin

Navigate to User Administration > Groups and create a new record (see table for field descriptions).

To see some of the fields, you may need to personalize the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the group.</td>
</tr>
<tr>
<td>Manager</td>
<td>Group manager or lead.</td>
</tr>
<tr>
<td>Type</td>
<td>Category for this group. For example, a group designated as type catalog is a service catalog group and can also be accessed under the Service Catalog &gt; Catalog Policy &gt; Fulfillment Groups module. You may need to personalize the form to add the Type field. Activating the Work Management plugin adds the Type field automatically.</td>
</tr>
<tr>
<td>Group email</td>
<td>Group email distribution list or the email address of the point of contact, such as the group manager.</td>
</tr>
<tr>
<td>Parent</td>
<td>Other group of which this group is a member. If a group has a parent, the child group inherits the roles of the parent group. The members of the child group are not members of the parent group. For example, if an incident is assigned to the parent group and you click the Assigned to lookup icon, only the members in the parent group are available. The members of the child group are not available.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box that indicates whether the group is active or inactive. Inactive groups still appear in any reference field that already references the group, but are not visible by non-admin users in:</td>
</tr>
<tr>
<td>Exclude manager</td>
<td>Check box that controls whether the group manager receives email notifications.</td>
</tr>
</tbody>
</table>

Note: ITIL is added for groups with an empty group type. Also, the default reference qualifier for tasks allows these groups to assign tasks and other task types to the group.
### Field | Description
--- | ---
Include members | Check box that controls whether the group members receive individual emails when someone sends an email to the Group Email address. The only exception to this functionality is for approval notifications, whereby all members of a group receive an approval notification, regardless of the Include members selection. See Receive notifications for more information.

| Description | Helpful information about the group.

### Add a user to a group

Add a user to a group so the user inherits all the roles assigned to the group.

Role required: user_admin

If you are a non-admin user, you cannot add a user to a group that contains the admin role. If you do not have a security_admin role, you cannot add a user to a group that contains the security_admin role.

1. Navigate to User Administration > Groups.
2. Click a group Name.
3. In the Group Members related list, click Edit.
4. Select one or more names in the Collection list.
5. Click Add.
6. Click Save.

### Remove a user from a group

Remove a user from a group when they change roles.

Role required: user_admin or itil

1. Navigate to User Administration > Groups.
2. Click a group Name.
3. In the Group Members related list, select the check box next to each group member name you wish to remove.
4. From the Actions on selected rows menu, select Delete.

**Note:** Before selecting Delete, first make sure you have properly selected the rows containing the specific users you wish to remove from the group.

### Hide groups

You can hide groups by introducing a hidden field to the group form and then creating a business rule to filter out groups marked as hidden.

Only users in the hidden group will be able to see the hidden field when selecting a group in a reference field.

### Add a hidden field to a group form

Add a custom check box field to the group form to allow the group to be hidden by the business rule.

Create a new true/false field labeled Hidden on the Group form.
The system creates a new field called `u_hidden` on the `[sys_user_group]` table and enables use of the Hidden check box to designate a hidden group.

**Add a business rule to filter out hidden groups**

After creating a custom field on the group form to hide the group, add a business rule to filter out hidden groups. Only users within the hidden group and users marked admin or groups_admin can see the group.

Create a new **before query** business rule on the `[sys_user_group]` (Group) table with the following script:

```javascript
if (!gs.hasRole("admin") && !gs.hasRole("groups_admin") && gs.getSession().isInteractive()) {
  var qc = current.addQuery("u_hidden", "!=", "true"); //cannot see hidden groups...
  qc.addOrCondition("sys_id", "javascript:getMyGroups()"); //...unless in the hidden group
}
```

**Configure group types for assignment groups**

Use the **Type** field to define categories of groups. Once defined, you can use these categories to filter assignment groups based on the group type using a reference qualifier.

For example, when selecting an assignment group from the Incident form, **Type** can be used to filter groups based on whether they are typically involved in the Incident management process. Groups such as Network or Help Desk are displayed as they are typically involved. Groups such as HR or New York are omitted.

The following items are provided in the base system.

- The types `catalog`, `itil`, and `survey`.
- The reference qualifier on `[task.assignment_group]` filters on `[Type] [equals] [null]`.
- A reference qualifier named `GetGroupFilter` is available to filter for group types using dynamic filters.

**Note:** Dictionary overrides allow administrators to filter for a group type on an extended table with a simple reference qualifier override.

**Add a new group type**

You can add additional group types to filter assignment groups for tasks.

Role required: admin

You may need to configure the form to display the **Type** field.

1. Navigate to **User Administration > Groups**.
2. Select a group record.
3. Click the lock icon beside **Type**.
4. Click the lookup icon beside the selection field. The Group Types dialog opens.
5. Complete the following steps.
   a) Click **New**.
   b) Enter the group type name and description.
      For example, to define a type for a group as `incident` and `problem`, enter: `incident,problem`. Click **Submit**.

The Group form reopens with the new type listed.

6. Optional: Add additional group types if needed.
7. Click **Update**.

**Assign a group type**

You can assign group types to filter assignment groups for tasks.

Role required: admin

1. Navigate to **User Administration > Groups** and select the desired group.
2. Click the lock icon beside **Type**.
3. Click the lookup icon beside the selection field and select one or more group types.

   **Note:** Because the default behavior of `task.assignment_group` is to filter out groups with group types defined, adding a type to a group filters it out of the **Assignment Group** field on tasks. To change the behavior, set up the reference qualifier.

4. Click **Update**.

**Roles**

Roles control access to features and capabilities in applications and modules. The admin role provides access to all features and capabilities.

After access has been granted to a role, all the groups or users assigned to the role are granted the access. Roles can contain other roles, and any access granted to a role is granted to any role that contains it.

For a complete list of the roles included with the ServiceNow platform, see **Base system roles**.

**Create a role**

Create a role to control access to features and capabilities in applications and modules. The new role does not have access to any application or module until you add other roles to it, or add it to the appropriate applications and modules.

Role required: admin

Once access has been granted to a role, all groups or users assigned to the role are granted the access. Roles can contain other roles, and any access granted to a role is granted to any role that contains it.

For a complete list of the roles included with the base instance, see **Base system roles**.

   **Note:** You cannot rename roles of any kind in the Now Platform. If you manually create a role, you cannot rename it once you save it.

1. Navigate to **User Administration > Roles** and create a new record.
2. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the role.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Requires Subscription</th>
<th>Indicates if users with this role require allocation to a subscription in the Subscription form in Subscription Management to stay in compliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Chargeable user role that requires allocation of users with this role to subscriptions. These user roles appear in the Associated Roles related list in the Subscription form when you associated with downloaded plugins for a subscription. To learn more, see Subscription form.</td>
</tr>
<tr>
<td>No</td>
<td>Not a chargeable role.</td>
</tr>
<tr>
<td>Unspecified</td>
<td>Neither</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application</th>
<th>Select the application that contains this record.</th>
</tr>
</thead>
</table>

| Elevated privilege | A role that requires elevated privilege prevents the system from assigning it to a user at login. Instead, a user must manually elevate privileges to receive the elevated role. Select this option to mark this role as required to elevate it to high security. See Elevated privilege roles for more information. |

<table>
<thead>
<tr>
<th>Description</th>
<th>Select the roles to delegate to the group member.</th>
</tr>
</thead>
</table>

### Grant a role access to applications and modules

Roles control access to features and capabilities in applications and modules. You add a role to an application or module to enable the role to grant access to the application or module for all users with the role.

**Role required: admin**

1. Navigate to **System Definition > Applications** or **System Definition > Modules**.
2. Click the appropriate application or module to open it in form view.
3. Click the lock to open the **Roles** field.
4. Use the slushbucket to add the desired roles to the application or module.
5. Click the lock to close the **Roles** field, and then save your changes.

### Create a group role

Create a group role to control access to features and capabilities in applications for all members in a group.

**Role required: admin**

1. Navigate to **User Administration > Group Roles**.
2. Click **New**.
3. Fill in the fields on the form and then click **Submit**.
### Add a role to an existing role

When you add a new role to an existing role for a user, the user inherits the access that is granted by the new role.

Role required: admin

1. Navigate to **User Administration > Roles** and open the existing role.
2. Click **Edit** in the Contains Roles related list.
3. Use the slushbucket to add one or more roles to the existing role.
4. Click **Save**.

The users with the existing role inherit the access that is granted by the new role.

### Assign a role to a group

You can assign a role to a group to grant access to applications and modules to group members.

Role required: user_admin or admin

When you assign roles to groups rather than to individual users, members of the group inherit the role. When a user switches groups, the new group role is assigned automatically. For information about the Service Mapping roles, see **Control user access to application services**.

1. Navigate to **User Administration > Groups**.
2. Click the group to assign a role.
3. In the **Roles** related list, click **Edit**.
4. Use the slushbucket to add the desired roles to the group.
5. Click **Save**.

### Assign a role to a user

A user inherits roles from all groups to which the user belongs. You can also assign roles directly to a user. Whenever a user is assigned a new role, it only takes effect after logging in with a new session.

Role required: user_admin or admin

To grant the admin role to a user, you must also have the admin role. To grant the security_admin role to a user, you must also have the security_admin role, and must elevate to the security_admin role before granting the security_admin role to other users. See **Elevate to a privileged role**.

You cannot delete roles that are assigned to the group from the user record. You must remove the user from the group record.

1. Navigate to **User Administration > Users** and then open a user record.
2. In the **Roles** related list, click **Edit**.
3. In the **Collection** list, select the desired roles, and then click **Add**.
4. Click **Save**.
### Base system roles

Administrators can assign one or more base system user roles to grant access to base system platform features and applications.

The following standard roles are included in the base ServiceNow system with a new instance.

**Note:** You cannot rename roles of any kind in the Now Platform.

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>The administrator role. This role has special access to all system features, functions, and data because administrators can override ACL rules and pass all role checks. Consider these implications when using admin overrides on ACLs. If you have sensitive information, such as HR records, that you need to protect, you must create a custom admin role for that area and train a person authorized to see those records to act as the administrator. Also note the Special Administrative Roles.</td>
</tr>
<tr>
<td>agent_admin</td>
<td>Can manage MID Server-related scripts.</td>
</tr>
<tr>
<td>ais_admin</td>
<td>Can query, create, update, and delete indexing and search settings and log messages through the AI Search application.</td>
</tr>
<tr>
<td>approval_admin</td>
<td>Can approve or reject approvals.</td>
</tr>
<tr>
<td>approver_user</td>
<td>Can modify requests for approval routed to them. They also have all capabilities of Requesters.</td>
</tr>
<tr>
<td>assignment_rule_admin</td>
<td>Can manage Assignment Rules.</td>
</tr>
<tr>
<td>asset</td>
<td>Can manage hardware and software assets.</td>
</tr>
<tr>
<td>catalog</td>
<td>Has access to service catalog requests.</td>
</tr>
<tr>
<td>catalog_admin</td>
<td>Can manage the Service Catalog application, including catalog categories and items.</td>
</tr>
<tr>
<td>catalog_editor</td>
<td>Can create, modify, and publish items within categories they are assigned to.</td>
</tr>
<tr>
<td>catalog_item_designer</td>
<td>Can view the status of their category requests.</td>
</tr>
<tr>
<td>catalog_manager</td>
<td>Can view and assign catalog editors to their categories. Can also create, modify, and publish items within their categories.</td>
</tr>
</tbody>
</table>

**Warning:** Grant this privilege carefully.
<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>category_manager</td>
<td>Can create, edit, and delete model categories.</td>
</tr>
<tr>
<td>cmdb_read</td>
<td>Can read any CMDB table. Contained in admin and itil.</td>
</tr>
<tr>
<td>communication_manager</td>
<td>Manages communication for major incidents and is responsible for communicating with all stakeholders.</td>
</tr>
<tr>
<td>contract_manager</td>
<td>Can create, edit, and delete contracts through the Contract Management application.</td>
</tr>
<tr>
<td>data_classification_admin</td>
<td>Administers all aspects of the Data Classification application, data classification code setup and assignment,</td>
</tr>
<tr>
<td>data_classification_auditor</td>
<td>Audits Data Classification code assignments.</td>
</tr>
<tr>
<td>ecmdb_admin</td>
<td>Can administer the CMDB.</td>
</tr>
<tr>
<td>filter_admin</td>
<td>Can manage filters.</td>
</tr>
<tr>
<td>filter_global</td>
<td>Can create global filters.</td>
</tr>
<tr>
<td>filter_group</td>
<td>Can create filters that belong to groups of which the user is a member.</td>
</tr>
<tr>
<td>gauge_maker</td>
<td>Can create gauges from reports. Starting with Helsinki, reports are no longer made into gauges.</td>
</tr>
<tr>
<td>guided_tour_admin</td>
<td>Can manage and administer Guided Tour functionality.</td>
</tr>
<tr>
<td>image_admin</td>
<td>Can manage image files on the Images [db_image] table.</td>
</tr>
<tr>
<td>impersonator</td>
<td>Can impersonate users. Does not allow impersonation of admin users.</td>
</tr>
<tr>
<td>import_admin</td>
<td>Can manage all aspects of import sets and imports.</td>
</tr>
<tr>
<td>import_scheduler</td>
<td>Can schedule imports.</td>
</tr>
<tr>
<td>import_set_loader</td>
<td>Can load import sets.</td>
</tr>
<tr>
<td>import_transformer</td>
<td>Can manage import set transform maps and run transforms.</td>
</tr>
<tr>
<td>incident_manager</td>
<td>Manages Incident properties and Major Incident trigger rules.</td>
</tr>
<tr>
<td>inventory_admin</td>
<td>Can create and delete stock information. Only users with the inventory_admin role can edit stock rules, stockrooms, and stockroom types.</td>
</tr>
<tr>
<td>inventory_user</td>
<td>Has access to stock information. Can create and manage transfer orders.</td>
</tr>
<tr>
<td>itil</td>
<td>Can perform standard actions for an ITIL helpdesk technician. Can open, update, close incidents, problems, changes, configuration management items. By default, only users with the itil role can have tasks assigned to them.</td>
</tr>
<tr>
<td>itil_admin</td>
<td>Possesses more privileges than the itil role and is intended for team leads. This role has the ability to delete incidents, problems, changes, and other related entities when both the itil and itil_admin roles are assigned.</td>
</tr>
<tr>
<td>knowledge</td>
<td>Can create, edit, and review knowledge base articles.</td>
</tr>
<tr>
<td>Role</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>knowledge_admin</td>
<td>Can manage the knowledge base.</td>
</tr>
<tr>
<td>list_updater</td>
<td>Can use Update Entire List and Update Selected menu options on lists.</td>
</tr>
<tr>
<td>maint</td>
<td>Reserved for ServiceNow use.</td>
</tr>
<tr>
<td>mid_server</td>
<td>Role that any MID server user should be granted. This role gives the MID server access to the tables it ordinarily uses.</td>
</tr>
<tr>
<td>model_manager</td>
<td>Can create new CMDB models. Model manager can control the base models and any model extensions that are not software or consumables. Consumable models are controlled by the asset manager role (asset). Software models are control by the software asset manager role (sam).</td>
</tr>
<tr>
<td>major_incident_manager</td>
<td>Initiates the major incident process by assessing and approving major incident candidates or creating a major incident. Maintains the ownership and accountability for the lifecycle of the incident. Identifies the users and groups to be involved in the resolution activities and sets up communication channels.</td>
</tr>
<tr>
<td>nobody</td>
<td>The nobody role means that no user has access - not even admin or maint. Use the nobody role carefully. The nobody role takes precedence over the admin override option on ACLs, so even admins cannot have access. See Create an ACL rule. Do not assign it to specific users. You can use this role in ACLs that control access to resources, such as UI pages, processors, script includes, and records. <strong>Warning:</strong> Applying the nobody role may be irreversible if applied to some important system functions.</td>
</tr>
<tr>
<td>personalize</td>
<td>Can configure forms, lists, rules, controls, scripts.</td>
</tr>
<tr>
<td>personalize_choices</td>
<td>Can configure choices and predefined responses for non-journal fields designated as choice or suggestion fields.</td>
</tr>
<tr>
<td>personalize_control</td>
<td>Can configure controls on lists, such as filters, links, and buttons.</td>
</tr>
<tr>
<td>personalize_dictionary</td>
<td>Can configure dictionary entries and labels.</td>
</tr>
<tr>
<td>personalize_form</td>
<td>Can configure forms.</td>
</tr>
<tr>
<td>personalize_list</td>
<td>Can configure lists and list calculations.</td>
</tr>
<tr>
<td>personalize_responses</td>
<td>Can configure predefined responses for journal fields designated as suggestion fields.</td>
</tr>
<tr>
<td>Role</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>personalize_rules</td>
<td>Can configure business rules and scripts. This role contains the following specialized roles for granting selective, administrative access to rules and scripts:</td>
</tr>
<tr>
<td></td>
<td>• business_rule_admin</td>
</tr>
<tr>
<td></td>
<td>• client_script_admin</td>
</tr>
<tr>
<td></td>
<td>• ui_policy_admin</td>
</tr>
<tr>
<td></td>
<td>• ui_action_admin</td>
</tr>
<tr>
<td>personalize_styles</td>
<td>Can configure field styles.</td>
</tr>
<tr>
<td>personalize_ui</td>
<td>Can configure forms and lists.</td>
</tr>
<tr>
<td>public</td>
<td>No login is required to access features or functions with the public role.</td>
</tr>
<tr>
<td>release_admin</td>
<td>Can edit Release history for a release.</td>
</tr>
<tr>
<td>report_admin</td>
<td>Can manage reports.</td>
</tr>
<tr>
<td>report_global</td>
<td>Can create global reports.</td>
</tr>
<tr>
<td>report_group</td>
<td>Can create reports and share reports with groups that the user is a member of. Users with this role can edit reports shared by other users in the group.</td>
</tr>
<tr>
<td>report_publisher</td>
<td>Can make reports available on a public page.</td>
</tr>
<tr>
<td>report_scheduler</td>
<td>Can schedule a report to be emailed.</td>
</tr>
<tr>
<td>script_fix_admin</td>
<td>Can manage fix scripts.</td>
</tr>
<tr>
<td>search_application_admin</td>
<td>Can query, create, update, and delete records on search UX-related tables. Contains the ais_admin role.</td>
</tr>
<tr>
<td>sn_appclient.app_client_company_installer</td>
<td>Can install applications containing the same company as the currently logged in instance. User role that allows for first time installation of only those applications for the company associated with the currently logged in instance. A user with this role cannot install an application for another company.</td>
</tr>
<tr>
<td>sn_appclient.app_client_user</td>
<td>Can install applications containing the same company as the currently logged in instance.</td>
</tr>
<tr>
<td>soap</td>
<td>Can query, create, update, and delete records on all tables, as well as execute scripts.</td>
</tr>
<tr>
<td>soap_create</td>
<td>Can create records on all tables and columns.</td>
</tr>
<tr>
<td>soap_delete</td>
<td>Can delete records on all tables and columns.</td>
</tr>
<tr>
<td>soap_ecc</td>
<td>Can query, create, and update on the ECC Queue table only.</td>
</tr>
<tr>
<td>soap_query</td>
<td>Can query records on all tables and columns.</td>
</tr>
<tr>
<td>soap_query_update</td>
<td>Can query and update records on all tables and columns.</td>
</tr>
<tr>
<td>soap_script</td>
<td>Can execute business rule endpoint function via script.do.</td>
</tr>
<tr>
<td>soap_update</td>
<td>Can update records on all tables and columns.</td>
</tr>
<tr>
<td>Role</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>survey_admin</td>
<td>Can manage survey masters, questions, and instances. Contains the assessment_admin role.</td>
</tr>
<tr>
<td>survey_reader</td>
<td>Can read survey instances and responses.</td>
</tr>
<tr>
<td>task_editor</td>
<td>Can edit protected task fields.</td>
</tr>
<tr>
<td>template_editor</td>
<td>Can create templates for personal use, and modify or delete personal templates. Included in the itil role in the base system.</td>
</tr>
<tr>
<td>template_editor_global</td>
<td>Can create templates for global use.</td>
</tr>
<tr>
<td>template_editor_group</td>
<td>Can create templates for groups.</td>
</tr>
<tr>
<td>template_scheduler</td>
<td>Can schedule template-based record creation.</td>
</tr>
<tr>
<td>text_search_admin</td>
<td>Can customize Global Text Search groups and tables.</td>
</tr>
<tr>
<td>timecard_admin</td>
<td>Can approve, modify, and delete the time cards of other users.</td>
</tr>
<tr>
<td>ts_admin</td>
<td>Can administer Zing text indexing and search engine.</td>
</tr>
<tr>
<td>unlimited_createnow</td>
<td>Role for CreateNow unlimited licensed users.</td>
</tr>
<tr>
<td>upgrade_app</td>
<td>Can upgrade installed applications containing the same company as the currently logged in instance. Cannot perform first time installations of applications published to the Application Client page.</td>
</tr>
<tr>
<td>user</td>
<td>Available for customer use, has no function in the base system.</td>
</tr>
<tr>
<td>user_admin</td>
<td>Can administer users, groups, locations, and companies.</td>
</tr>
<tr>
<td>view_changer</td>
<td>Can switch active views.</td>
</tr>
<tr>
<td>workflow_admin</td>
<td>Can create, edit, publish or delete graphical workflows.</td>
</tr>
<tr>
<td>workflow_creator</td>
<td>Can create new graphical workflows.</td>
</tr>
<tr>
<td>workflow_publisher</td>
<td>Can publish graphical workflows.</td>
</tr>
</tbody>
</table>

**Special administrative roles**

Certain roles grant specific administrative rights without the full privileges of the admin role. For example, an administrator can grant a user the right to change UI policy but not client scripts.

These roles do not change the behavior of the admin role, which grants full administrative privileges.

**Note:** You cannot rename roles of any kind in the Now Platform.

**Special administrative roles**

<table>
<thead>
<tr>
<th>Role</th>
<th>Privilege</th>
</tr>
</thead>
<tbody>
<tr>
<td>assignment_rule_admin</td>
<td>Allows management of Assignment Rules.</td>
</tr>
<tr>
<td>ui_script_admin</td>
<td>Allows management of UI Scripts.</td>
</tr>
</tbody>
</table>
Read-only role

The read-only role (snc_read_only) restricts a user or a group of users to read-only access on the tables to which the user already has access.

This role is not intended to be the only role a user has. It is intended to be an extra role to restrict insert, update, and delete operations on the tables that the user can access as defined by the other roles.

After you assign this role to a user, they can no longer create, update, or delete records on ANY tables.

Note: Assign this role only to users. Do not assign this role to other resources in the system, including applications, ACLs, and so on.

The snc_read_only role can be assigned to any user to limit access to data without having to create ACLs for system tables, custom tables and fields. This practice is useful for performing internal or external audits without allowing a user to have insert or update access to data.

Users with the snc_read_only role have the following restrictions regardless of other roles and privileges they have.

- Cannot insert, update, or delete records from the UI or when using the GlideRecord API.
- Cannot activate or upgrade plugins.
- Cannot directly run SQL.
- Cannot upload XML files.
- Can only run background scripts when on an instance in the public sandbox environment.

Note: These role restrictions are in place even if impersonating another user with write access such as an admin.

Activate the read-only role

If it is not already active, an administrator can activate the Read-Only User Role (com.snc.read_only.role) plugin.

Role required: admin

1. Navigate to System Applications > All Available Applications > All.
2. Find the Read-Only User Role (com.snc.read_only.role) plugin using the filter criteria and search bar.
   You can search for the plugin by its name or ID. If you cannot find a plugin, you might have to request it from ServiceNow personnel. For more information, see Request a plugin.
3. Click Install, and then in the Activate Plugin dialog box, click Activate.
Read-only role properties

These system properties control the snc_read_only role. The following default values are used for the properties.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| glide.security.snc_read_only_role.tables.exempt_create | Specifies which tables are exempt from the read-only role enforcement and allow the creation of new records.  
- Type: string  
- Default value: sys_user_session, sysevent, syslog, syslog_transaction, sys_user_preference, sys_ui_list, sys_ui_list_element, sys_db_cache, user_multifactor_auth  
- Location: System Properties [sys_properties] table |
| glide.security.snc_read_only_role.tables.exempt_write | Specifies which tables are exempt from the read-only role enforcement and allow the updating of existing records.  
- Type: string  
- Default value: sys_user_session, sysevent, syslog, syslog_transaction, sys_user_preference, sys_ui_list, sys_ui_list_element, sys_db_cache, user_multifactor_auth  
- Location: System Properties [sys_properties] table |
| glide.security.snc_read_only_role.tables.exempt_delete | Specifies which tables are exempt from the read-only role enforcement and allow the deletion of existing records.  
- Type: string  
- Default value: sys_user_preference, sys_ui_list, sys_ui_list_element, sys_db_cache, user_multifactor_auth  
- Location: System Properties [sys_properties] table |

After you configure these properties, assign the read-only role as needed. When users log in, they are restricted from creating, updating, or deleting records on ANY tables unless you modified these properties.

Note: Test the read-only role by assigning it to a user and then impersonating that user.
Delegating roles

Administrators can authorize users to be role delegators to assign roles to users who are in a particular group. Role delegators can assign only the roles that are assigned to them.

Role delegation and record producers

These graphical workflows include the following:

- Grant role_delegator role to user in group
- Delegate roles to group member

These workflows can be customized as desired to add approval steps.

Group manager change business rule

The Group Manager Change business rule, which is disabled by default, automatically grants the role_delegator role to a user who is designated manager of a group in the Manager field on the Group form. The role is removed when the user is no longer the manager of the group.

Activate the business rule to take advantage of it.

View delegated roles

An administrator can view role designation in user records, the Role Delegators module, or the Role Audit module.

User records

Open a user record by navigating to User Administration > Users and selecting the user. You can see all the roles assigned to that user in the Roles related list.

Role Delegators module

To view existing role delegators and the groups in which they can delegate roles, navigate to User Administration > Role Delegators.

Role Audit module

The Audit Role list view displays all the role changes made in the instance by user and group. To access the Audit Role list, navigate to System Security > Reports > Role Audit.

Define role delegators and delegate roles

You can designate role delegators. A role delegator can assign roles to users who are in a particular user group.

Role required: admin to define role delegators, and role_delegator to delegate roles

The roles that delegators can assign to other users include the roles that the delegator inherits from a group and those roles that the administrator assigns to the delegator.

1. Navigate to User Administration > Designate Role Delegator.
2. Select the group that includes the user who you want to be the role delegator.
3. Select the user.
4. Click **Submit**.
   A change request for the role delegator request is created and automatically approved.

5. If you are a role delegator, complete the following steps to delegate a role.
   a) Navigate to **User Administration > Delegate Roles in Group** and fill out the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Input Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group</td>
<td>Select the group in which to delegate a role or roles to a member. Any group can be selected, including groups that the role_delegator does not belong to or groups that the role_delegator does not manage.</td>
</tr>
<tr>
<td>User</td>
<td>Select the group member to delegate a role or roles.</td>
</tr>
<tr>
<td>Roles to delegate</td>
<td>Select the roles to delegate to the group member. The roles available for delegating are only the roles that the role_delegator has.</td>
</tr>
</tbody>
</table>

   b) Click **Submit**.

   Upon submission, a change request is created for the delegation request. This change request is approved automatically, and the specified roles are granted to the named user in the group selected.

   Delegated roles can be removed in the same form by reversing the process. Select the group and user, remove the unwanted roles from the Roles slushbucket, and then resubmit the request.

   c) Optional: To remove a delegated role from a user, open the delegation record and remove the unwanted role or roles.

**Prevent a role from being delegated**

You can prevent roles from being delegated to users.

Role required: admin

By default, the following roles cannot be delegated.

- admin
- public
- nobody
- role_delegator, a user with the role_delegator role cannot delegate this role to other group members

1. Navigate to **User Administration > Roles**.
2. Open the role.
3. Configure the form to add the **Grantable** or **Can delegate** fields.
4. Clear the check box for one or both of these fields.
5. Click **Update**.

**Security jump start - ACL rules**

The Security Jump Start (ACL Rules) Plugin is installed automatically on all new instances.
**Note:** The Security Jump Start (ACL Rules) plugin is required for the following functionality. The plugin is automatically installed for new instances.

These rules were written to provide a jump start on securing many system tables, to make it easier for an organization to more quickly get into production.

This plugin is not intended for existing instances, as it might modify security access to tables that are already in use in a production environment. If an admin is interested in the new ACL rules provided by this plugin, one or more of them may be created manually in an existing instance as specific needs dictate. This list of ACLs may be used as a guideline in that case. Should an admin strongly want this plugin installed on an existing instance, we highly recommend the plugin be tested extensively in a test instance first, to ensure that the rules do not conflict with the operational needs of the organization's current implementation.

The following ACLs are included in this plugin. Click the icon in a header row to sort that column in ascending or descending order. The Operation key is as follows:

- **R**=read
- **W**=write
- **D**=delete
- **C**=create

<table>
<thead>
<tr>
<th>Name</th>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cmdb_ci</td>
<td>WCD</td>
<td>asset or itil role required to write/create/delete Configuration Item records</td>
</tr>
<tr>
<td>cmn_department</td>
<td>WD</td>
<td>user_admin role required to write/delete Department records</td>
</tr>
<tr>
<td>cmn_location</td>
<td>WC</td>
<td>user_admin role required to write/create Location records</td>
</tr>
<tr>
<td>core_company</td>
<td>WD</td>
<td>user_admin role required to write/delete Company records</td>
</tr>
<tr>
<td>kb_knowledge</td>
<td>create</td>
<td>knowledge role required to created Knowledge records</td>
</tr>
<tr>
<td>ldap_ou_config</td>
<td>RWCD</td>
<td>user_admin role required to read/write/create/delete LDAP OU Definition records</td>
</tr>
<tr>
<td>ldap_server_config</td>
<td>RWCD</td>
<td>user_admin role required to read/write/create/delete LDAP Server records</td>
</tr>
<tr>
<td>process_guide</td>
<td>WCD</td>
<td>admin role required to write/create/delete Process Guide records</td>
</tr>
<tr>
<td>process_step</td>
<td>WCD</td>
<td>admin role required to write/create/delete Process Step records</td>
</tr>
<tr>
<td>sc_category</td>
<td>create</td>
<td>catalog_admin role required to create Service Catalog Category records</td>
</tr>
<tr>
<td>sc_category</td>
<td>delete</td>
<td>catalog_admin role required to delete Service Catalog Category records</td>
</tr>
<tr>
<td>sc_category</td>
<td>write</td>
<td>catalog_admin role required to write to Service Catalog Category records</td>
</tr>
<tr>
<td>Name</td>
<td>Operation</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>sc_cat_item</td>
<td>write</td>
<td>catalog_admin role required to write to Catalog Item records</td>
</tr>
<tr>
<td>sc_cat_item</td>
<td>delete</td>
<td>catalog_admin role required to delete Catalog Item records</td>
</tr>
<tr>
<td>sc_cat_item</td>
<td>create</td>
<td>catalog_admin role required to create Catalog Item records</td>
</tr>
<tr>
<td>sysevent_email_action</td>
<td>read</td>
<td>all users can read Email Notification records (for subscription purposes)</td>
</tr>
<tr>
<td>sysevent_register</td>
<td>RWCD</td>
<td>admin role required to read/write/create/delete Event Registry records</td>
</tr>
<tr>
<td>sysevent_script_action</td>
<td>RWCD</td>
<td>admin role required to read/write/create/delete Script Action records</td>
</tr>
<tr>
<td>syslog</td>
<td>RWCD</td>
<td>admin required to read/write/create/delete Log Entry records</td>
</tr>
<tr>
<td>sysrule</td>
<td>RWCD</td>
<td>admin required to read/write/create/delete Rule records (Email Notifications, Inbound Email Actions, Approval Rules, etc.)</td>
</tr>
<tr>
<td>sysrule</td>
<td>read</td>
<td>all users can read Email Notification records for (subscription based notifications)</td>
</tr>
<tr>
<td>sys_app_application</td>
<td>WCD</td>
<td>admin required to write/create/delete Application records</td>
</tr>
<tr>
<td>sys_app_category</td>
<td>WCD</td>
<td>admin role required to write/create/delete Application Category records</td>
</tr>
<tr>
<td>sys_app_module</td>
<td>WCD</td>
<td>admin required to write/create/delete Module records</td>
</tr>
<tr>
<td>sys_audit</td>
<td>RWCD</td>
<td>admin required to read/write/create/delete Audit records</td>
</tr>
<tr>
<td>sys_dictionary</td>
<td>RWC</td>
<td>personalize_dictionary role required to read/write/create Dictionary records</td>
</tr>
<tr>
<td>sys_dictionary.*</td>
<td>read</td>
<td>personalize_dictionary role can read Dictionary fields</td>
</tr>
<tr>
<td>sys_documentation</td>
<td>delete</td>
<td>personalize_dictionary role required to delete Field Label records</td>
</tr>
<tr>
<td>sys_documentation</td>
<td>create</td>
<td>personalize_dictionary role required to create Field Label records</td>
</tr>
<tr>
<td>sys_documentation</td>
<td>write</td>
<td>personalize_dictionary role required to write Field Label records</td>
</tr>
<tr>
<td>sys_gauge</td>
<td>RWCD</td>
<td>admin role required to read/write/create/delete Gauge records</td>
</tr>
<tr>
<td>sys_gauge_count</td>
<td>RWCD</td>
<td>admin role required to read/write/create/delete Gauge Count records</td>
</tr>
<tr>
<td>Name</td>
<td>Operation</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>sys_group_has_role</td>
<td>read</td>
<td>itil role required to see Group Role records</td>
</tr>
<tr>
<td>sys_home</td>
<td>WCD</td>
<td>itil_admin role required to write/create/delete Welcome Page Section records</td>
</tr>
<tr>
<td>sys_installation_exit</td>
<td>WCD</td>
<td>admin role required to write/create/delete Installation Exit records</td>
</tr>
<tr>
<td>sys_job</td>
<td>WCD</td>
<td>admin role required to write/create/delete Sys Job records</td>
</tr>
<tr>
<td>sys_nav_link</td>
<td>WCD</td>
<td>admin role required to write/create/delete Navigation Link records</td>
</tr>
<tr>
<td>sys_perspective</td>
<td>WCD</td>
<td>admin role required to write/create/delete Menu List records</td>
</tr>
<tr>
<td>sys_portal</td>
<td>RWCD</td>
<td>admin role required to read/write/create/delete Portal records</td>
</tr>
<tr>
<td>sys_portal_page</td>
<td>RWCD</td>
<td>admin role required to read/write/create/delete Homepage records</td>
</tr>
<tr>
<td>sys_portal_preferences</td>
<td>RWCD</td>
<td>admin role required to read/write/create/delete Portal Preferences records</td>
</tr>
<tr>
<td>sys_processor</td>
<td>WC</td>
<td>admin role required to write/create Processor records</td>
</tr>
<tr>
<td>sys_properties</td>
<td>WC</td>
<td>admin role required to write/create System Property records</td>
</tr>
<tr>
<td>sys_properties_category</td>
<td>WCD</td>
<td>admin role required to write/create/delete Property Category records</td>
</tr>
<tr>
<td>sys_report</td>
<td>delete</td>
<td>roles that can delete Report records (does not restrict deleting through Report UI)</td>
</tr>
<tr>
<td>sys_report</td>
<td>write</td>
<td>roles that can write to Report records (does not restrict editing through Report UI)</td>
</tr>
<tr>
<td>sys_report</td>
<td>read</td>
<td>users can read their own Report records, those of their groups, and GLOBAL ones (does not affect viewing through Report UI)</td>
</tr>
<tr>
<td>sys_report</td>
<td>read</td>
<td>roles that can read Report records (does not restrict viewing through Report UI)</td>
</tr>
<tr>
<td>sys_reportroles</td>
<td>read</td>
<td>admin role required to read Report Roles records</td>
</tr>
<tr>
<td>sys_script</td>
<td>WCD</td>
<td>admin role required to write/create/delete Business Rule records</td>
</tr>
<tr>
<td>sys_script_ajax</td>
<td>WCD</td>
<td>admin role required to write/create/delete AJAX Script records</td>
</tr>
<tr>
<td>Name</td>
<td>Operation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>sys_script_client</td>
<td>WCD</td>
<td>admin role required to write/create/delete Client Script records</td>
</tr>
<tr>
<td>sys_script_include</td>
<td>WCD</td>
<td>admin role required to write/create/delete Script Include records</td>
</tr>
<tr>
<td>sys_security_acl</td>
<td>write</td>
<td>admin role required to write to Access Control records</td>
</tr>
<tr>
<td>sys_security_acl_role</td>
<td>create</td>
<td>admin role required to create Access Roles records</td>
</tr>
<tr>
<td>sys_security_acl_role</td>
<td>delete</td>
<td>admin role required to delete Access Roles records</td>
</tr>
<tr>
<td>sys_security_acl_role</td>
<td>write</td>
<td>admin role required to write to Access Roles records</td>
</tr>
<tr>
<td>sys_security_operation</td>
<td>delete</td>
<td>admin role required to delete Security Operation records</td>
</tr>
<tr>
<td>sys_security_operation</td>
<td>create</td>
<td>admin role required to create Security Operation records</td>
</tr>
<tr>
<td>sys_security_operation</td>
<td>write</td>
<td>admin role required to write to Security Operation records</td>
</tr>
<tr>
<td>sys_security_type</td>
<td>write</td>
<td>admin role required to write to Security Type records</td>
</tr>
<tr>
<td>sys_security_type</td>
<td>create</td>
<td>admin role required to create Security Type records</td>
</tr>
<tr>
<td>sys_security_type</td>
<td>delete</td>
<td>admin role required to delete Security Type records</td>
</tr>
<tr>
<td>sys_status</td>
<td>create</td>
<td>admin role required to create System Status records</td>
</tr>
<tr>
<td>sys_status</td>
<td>delete</td>
<td>admin role required to delete System Status records</td>
</tr>
<tr>
<td>sys_status</td>
<td>write</td>
<td>admin role required to write to System Status records</td>
</tr>
<tr>
<td>sys_template</td>
<td>write</td>
<td>template_editor role required to write to Template records</td>
</tr>
<tr>
<td>sys_template</td>
<td>create</td>
<td>template_editor role required to create Template records</td>
</tr>
<tr>
<td>sys_template</td>
<td>delete</td>
<td>template_editor role required to delete Template records</td>
</tr>
<tr>
<td>sys_template</td>
<td>read</td>
<td>template_editor role required to read Template Roles records</td>
</tr>
<tr>
<td>sys_ui_action</td>
<td>create</td>
<td>admin role required to create UI Action records</td>
</tr>
<tr>
<td>sys_ui_action</td>
<td>delete</td>
<td>admin role required to delete UI Action records</td>
</tr>
<tr>
<td>Name</td>
<td>Operation</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>sys_ui_action</td>
<td>write</td>
<td>admin role required to write to UI Action records</td>
</tr>
<tr>
<td>sys_ui_action_view</td>
<td>write</td>
<td>admin role required to write to UI View Action records</td>
</tr>
<tr>
<td>sys_ui_action_view</td>
<td>create</td>
<td>admin role required to create UI View Action records</td>
</tr>
<tr>
<td>sys_ui_action_view</td>
<td>delete</td>
<td>admin role required to delete UI View Action records</td>
</tr>
<tr>
<td>sys_ui_policy</td>
<td>create</td>
<td>admin role required to create UI Policy records</td>
</tr>
<tr>
<td>sys_ui_policy</td>
<td>delete</td>
<td>admin role required to delete UI Policy records</td>
</tr>
<tr>
<td>sys_ui_policy</td>
<td>write</td>
<td>admin role required to write to UI Policy records</td>
</tr>
<tr>
<td>sys_ui_policy_action</td>
<td>create</td>
<td>admin role required to create UI Policy Action records</td>
</tr>
<tr>
<td>sys_ui_policy_action</td>
<td>delete</td>
<td>admin role required to delete UI Policy Action records</td>
</tr>
<tr>
<td>sys_ui_policy_action</td>
<td>write</td>
<td>admin role required to write to UI Policy Action records</td>
</tr>
<tr>
<td>sys_ui_script</td>
<td>write</td>
<td>admin role required to write to UI Script records</td>
</tr>
<tr>
<td>sys_ui_script</td>
<td>delete</td>
<td>admin role required to delete UI Script records</td>
</tr>
<tr>
<td>sys_ui_script</td>
<td>create</td>
<td>admin role required to create UI Script records</td>
</tr>
<tr>
<td>sys_user</td>
<td>write</td>
<td>Users with no role cannot update any user record but their own</td>
</tr>
<tr>
<td>sys_user_grmember</td>
<td>delete</td>
<td>user_admin role required to delete Group Member records</td>
</tr>
<tr>
<td>sys_user_grmember</td>
<td>write</td>
<td>user_admin role required to write to Group Member records</td>
</tr>
<tr>
<td>sys_user_group</td>
<td>create</td>
<td>Only itil and above can create group records</td>
</tr>
<tr>
<td>sys_user_group</td>
<td>write</td>
<td>Only itil and above can create group records</td>
</tr>
<tr>
<td>sys_user_has_role</td>
<td>read</td>
<td>itil role required to see User Role records</td>
</tr>
<tr>
<td>sys_user_role</td>
<td>create</td>
<td>admin role required to create Role records</td>
</tr>
<tr>
<td>sys_user_role</td>
<td>delete</td>
<td>admin role required to delete Role records</td>
</tr>
<tr>
<td>Name</td>
<td>Operation</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>sys_user_role</td>
<td>write</td>
<td>admin role required to write to Role records</td>
</tr>
<tr>
<td>sys_user_role_contains</td>
<td>read</td>
<td>itil role required to see Contained Role records</td>
</tr>
<tr>
<td>sys_user_role_contains</td>
<td>write</td>
<td>admin role required to write to Contained Role records</td>
</tr>
<tr>
<td>sys_user_token</td>
<td>RWCD</td>
<td>admin role required to read/write/create/delete User Token records</td>
</tr>
</tbody>
</table>

**Note:** To learn more about this plug, see Security jump start (ACL rules) (instance security hardening) in Instance Security Hardening Settings.

### Audit user roles

Changes to user roles are automatically tracked in the Audit Roles [sys_audit_role] table.

Role required: admin

**Note:** If the Contextual Security: Role Management V2 plugin is installed, you must Enable role auditing with Contextual Security: Role Management V2.

Navigate to the Audit Roles [sys_audit_role] table.

The Audit Roles table displays changes to user roles.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Changed by</td>
<td>The user who made the change.</td>
</tr>
<tr>
<td>Count after change</td>
<td>Direct role added as a result of the change (if any), plus the number of inherited roles added.</td>
</tr>
<tr>
<td>Granted by group</td>
<td>If the role was inherited, the group that the role was inherited from.</td>
</tr>
<tr>
<td>Operation</td>
<td>The type of change. Values include:</td>
</tr>
<tr>
<td></td>
<td>• Added</td>
</tr>
<tr>
<td></td>
<td>• Removed</td>
</tr>
<tr>
<td>Role</td>
<td>The affected role.</td>
</tr>
<tr>
<td>User</td>
<td>The affected user.</td>
</tr>
</tbody>
</table>

### Non-interactive sessions

The Non-Interactive Sessions plugin creates a distinction between interactive and non-interactive users.

**Interactive users**

New users added to the instance automatically become interactive users. Interactive users can perform the following actions:
• Use their user name and password to log in to the UI or a service portal.
• Connect to an instance from a URL that calls a UI page, form, or list, for example, https://<instance name>.service-now.com/incident.do.
• Connect with single sign-on, for example, digest authentication or SAML.
• Use their credentials to authorize SOAP connections if allowed by strict security.
• Use their credentials for other API connections such as WSDL, JSON, XML, or XSD without restriction.

Non-interactive users

Non-interactive users can only use their credentials to authorize API connections such as JSON, SOAP, and WSDL. They cannot log in to the ServiceNow UI. The strict security high security setting determines if non-interactive users are subject to Contextual Security requirements.

Distinguishing between interactive and non-interactive users increases instance security by ensuring that users conform to the principle of least privilege.

Installed with Non-Interactive Sessions

Note: Non-Interactive Sessions is enabled for all new instances since the Calgary release. If you do not see it in the list of plugins, request it using the Activate Plugin service catalog item in Now Support.

• Adds a column Web Service Access Only [web_service_access_only] to the User [sys_user] table.
• Changes all existing users to be interactive users (web_service_access_only=false).
• Updates the User form to display the Web Service Access Only [web_service_access_only] field by default.

Create a non-interactive user for web services

Non-interactive users can only connect to a ServiceNow instance from an API protocol. Use this feature to set up user accounts for web service authentication purposes.

Role required: user_admin or admin

Non-interactive users cannot log in to an instance or a service portal or connect through single-sign-on, but can be used as a MID Server user if they are flagged as an Internal Integration User.

1. Navigate to User Administration > Users.
2. Search for the user to be updated.
   For example, SOAP user.
3. Select the Web Service Access Only check box.
4. Click Update.

Note:
The ServiceNow platform always uses any user name and password credentials supplied with a request even if the High Security Settings do not require authorization for a given API protocol. For example, if a SOAP request supplies a user name and password, the instance verifies those credentials even if SOAP requests do not require authorization. To avoid verifying user credentials, the request must not include them.
Make a non-interactive user record interactive

Manually switch a non-interactive user to an interactive user.

Role required: user_admin or admin

1. Navigate to User Administration > Users.
2. Search for the user you want to update. For example, System Administrator.
3. Clear the Web Service Access Only check box.
4. Click Update.

Update web service user accounts for strict security

If your instance requires strict security, add the soap role to any user accounts used for web services.

Role required: user_admin or admin

1. Navigate to User Administration > Users.
2. Select a web service user from the list.
3. From the Roles related list, click Edit.
4. Add soap to the Roles List.
5. Click Save.
6. Click Update.

Require authentication

You can specify whether non-interactive sessions require authentication from the High Security Settings module.

Role required: admin with elevated privileges

A non-interactive session bypasses the UI to connect to the instance at an API level. Typically, non-interactive sessions use set protocols such as JSON, SOAP, XSD, or WSDL. By default, all non-interactive sessions require authentication.

1. Log in with an administrator user with the security_admin role.
2. Elevate your privileges to use security_admin.
4. Select the matching Requires authorization... option for the protocol you want to set. For example, Requires authorization for incoming SOAP requests.
5. Select the check box to require authentication for the non-interactive session method. Clear the check box to allow the non-interactive session method to connect without providing any credentials.

Note: Activating the Non-Interactive Sessions plugin on an existing system may prevent any existing users that authorize SOAP and WSDL-based integrations from logging in unless they already have the soap role.

Instance Usage

The Instance Usage modules track usage for ServiceNow applications and for ServiceNow Store apps.

The usage analytics process collects data on all your instances and regularly updates the reports in the Application Usage Overview and ServiceNow Store Usage Overview modules. Application usage data is collected whenever an application is opened, and counts on tables are collected once a day. Data is collected on:
- The number of active users in the system
- The hardware CIs discovered (for instances that use Discovery)
- The number of cloud management service catalog items available to users in instances that use Cloud Management

Users with the admin or usage_admin role can view Application Usage Overview and ServiceNow Store Usage Overview reports.

**Application Usage Overview reports**

The Application Usage Overview module displays reports on the use of ServiceNow applications and ServiceNow Store applications on your instance.

See the illustration for tips on using the charts. Navigate to **Instance Usage > Application Usage Overview** and **Instance Usage > ServiceNow Store Usage Overview** to view the following reports and charts.

### Application Usage Overview reports

<table>
<thead>
<tr>
<th>Chart or report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Usage of ServiceNow Applications and Usage of ServiceNow Store Applications</td>
<td>Shows the number of views or operations performed for each of the listed applications, grouped by month.</td>
</tr>
<tr>
<td>Users of ServiceNow Applications and Users of ServiceNow Store Applications</td>
<td>Shows the number of active users who have used the instance, grouped by month. An active user is any user who could have accessed the applications, not only users who actually did access the applications.</td>
</tr>
<tr>
<td>Usage of Custom Applications</td>
<td>Shows the number of views or operations performed for each of the listed custom applications, grouped by month.</td>
</tr>
<tr>
<td>Users of Custom Applications</td>
<td>Shows the number of active users who have used custom applications, grouped by month. An active user is any user who could have accessed the custom applications, not only users who actually did access the applications.</td>
</tr>
<tr>
<td>Chart or report</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| **Additional Metrics** | Shows any of the following items, depending on your licensing agreement:  
  • Size of the primary database in the instance  
  • Performance analytics of all indices  
  • NotifyNow messages  
  • Discovery plugin active  
  • Password reset plugin active  
  • Cloud management — VMWare instance  
  • Vendor custom applications  
  • Custom applications  
  • Event management plugin active  
  • Active benchmark indicators  
  • Customer updated PA indicator  
  • Active users  
  • Cloud management — EC2 instances  
  • Orchestration core plugins active  
  • Custom tables extending out-of-box tables other than Task  
  • Virtual node count  
  • Active users for subscriptions  
  • NotifyNow conference calls  
  • Number of Google map page hits during the current month  
  • ServiceNow Edge Encryption plugins active  
  • Physical node count  
  • Cloud provisioning plugins active |
Working with charts on the Application Usage Overview report

- Click to add content like gauges, labels, or clocks to the chart.
- Save the chart as an image.
- Point to a data point to view details.
- Click a data point to view the underlying data.
- Click to view data for applications during the specified month.
- Refresh, Configure, or Close the chart.
Authentication

ServiceNow authentication validates the identity of a user who accesses an instance, and then authorizes the user to features that match the user's role or job function.

Available authentication methods

You can use several different methods to authenticate users. User credentials are matched to different saved credentials for each method.

Note: The OKTA SSO plugin has been deprecated.

Note: To learn more about the security properties that affect authorization processing, see Access Control in Instance Security Hardening Settings.

<table>
<thead>
<tr>
<th>Authentication methods</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local database</td>
<td>Username and password in their user record in the instance database.</td>
</tr>
<tr>
<td>External Single Sign-on (SSO)</td>
<td>Username and password configured in identity providers, which have a matching user account in the database.</td>
</tr>
<tr>
<td>LDAP</td>
<td>Username and password in their LDAP account, which has a matching user account in the database.</td>
</tr>
<tr>
<td>OAuth 2.0</td>
<td>Username and password of OAuth identity provider, which has a matching user account in the database.</td>
</tr>
<tr>
<td>Digest Token</td>
<td>Encrypted digest of the username and password in the user record.</td>
</tr>
<tr>
<td>Multifactor</td>
<td>Username and password in the database and a passcode sent to the user's mobile device that has Google Authenticator installed.</td>
</tr>
<tr>
<td>Adaptive authentication</td>
<td>Policy framework that uses authentication policies to evaluate access requests</td>
</tr>
<tr>
<td>Certificate based authentication</td>
<td>Unique PEM encoded certificates mapped to users instead of user name and password</td>
</tr>
</tbody>
</table>

Note: You can use SAML and Digest Authentication through the Multiple Provider SSO application.

External single sign-on (SSO)

External SSO allows organizations to use several SSO identity providers (IdPs) to manage authentication as well as retain local database (basic) authentication.

The integration supports any combination of local and external authentication methods on a single instance:

• LDAP
• SAML 2.0
• Digest Authentication
• OpenID Connect
• Local database authentication

For example, a globally dispersed corporation might require one SSO provider for their employees, a different one for their vendors, and local database authentication for their administrators. Alternatively, a company might implement SAML 2.0 and a digest token authentication solutions on the same instance.

Multi-Provider SSO properties, tables, and scripts

The Integration - Multiple Provider Single Sign-On Installer plugin includes the following system properties, tables, and scripts.

Properties

Multi-Provider SSO adds the following system properties.

Multi-Provider SSO properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.authenticate.auth.validate.url</td>
<td>Enables (true) or disables (false) the URL for the multi-provider SSO integration. This must be set to false if the instance is upgraded and SSO is not working in order to check the SAML script.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: false</td>
</tr>
<tr>
<td>glide.authenticate.multisso.debug</td>
<td>Enables (true) or disables (false) debug logging for the multi-provider SSO integration.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: false</td>
</tr>
<tr>
<td>glide.authenticate.multisso.enabled</td>
<td>Enables (true) or disables (false) multi-provider SSO.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: false</td>
</tr>
</tbody>
</table>

Tables

Multi-Provider SSO adds the following tables.

Multi-Provider SSO tables

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSO Properties [sso_properties]</td>
<td>Stores data for each IdP, schema, common SSO data, and so on.</td>
</tr>
<tr>
<td>SAML 2 Update 1 Properties</td>
<td>Stores data for SAML 2.0 Update 1 configurations such as SAML certificates.</td>
</tr>
<tr>
<td>Digest Properties [digest_properties]</td>
<td>Stores data for digest token authentication configurations.</td>
</tr>
</tbody>
</table>
### Scripts

Multi-Provider SSO adds the following scripts.

**Multi-Provider SSO scripts**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MultiSSO</td>
<td>Allows a customer to have an SSO type defined on a company basis.</td>
</tr>
<tr>
<td>MultiSSOLogin</td>
<td>Allows each domain to have their own login script.</td>
</tr>
<tr>
<td>MultiSSOLogout</td>
<td>Allows each domain to have their own logout script.</td>
</tr>
<tr>
<td>MultiSSO_OIDC_custom</td>
<td>Allows a user to define a custom Single Sign-on script for OIDC connection.</td>
</tr>
<tr>
<td>MultiSSO_OIDC_logout_custom</td>
<td>Allows a user to define a custom logout script for OIDC connection.</td>
</tr>
<tr>
<td>MultiSSO_Abstract_Core</td>
<td>Provides a base class for all multi-provider SSO classes.</td>
</tr>
<tr>
<td>MultiSSO_ClientHelper</td>
<td>Provides a client callable utility functions for multi-provider SSO.</td>
</tr>
<tr>
<td>MultiSSO_DigestedToken</td>
<td>Provides a base system logic for digested token authentication.</td>
</tr>
<tr>
<td>MultiSSO_SAML2_Update1</td>
<td>Provides logic to process SAML 2.0 Update 1 authentication for a multi-tenant single sign-on.</td>
</tr>
</tbody>
</table>

### Activate Multi-Provider SSO plugin

This integration requires the Integration - Multiple Provider Single Sign-On Installer (com.snc.integration.sso.multi.installer) plugin.

Role required: admin

1. Navigate to **System Applications > All Available Applications > All.**
2. Find the Integration - Multiple Provider Single Sign-On Installer (com.snc.integration.sso.multi.installer) plugin using the filter criteria and search bar.
   - You can search for the plugin by its name or ID. If you cannot find a plugin, you might have to request it from ServiceNow personnel. For more information, see Request a plugin.
3. Click **Install**, and then in the Activate Plugin dialog box, click **Activate**.

**Note:** When domain separation and delegated admin are enabled in an instance, the administrative user must be in the **global** domain. Otherwise, the following error appears: Application installation is unavailable because another operation is running: Plugin Activation for <plugin name>.
Set up Multi-Provider SSO

You must perform several steps to set up Multi-Provider SSO, including configuring properties, creating identity providers (IdPs), and configuring users to use SSO.

Multi-Provider SSO (SAML) IdP authentication flow
Describes the different entities that can authenticate a user through the SAML multi-SSO.

You can follow the authentication flow to understand when an entity authenticates a user using Multi-SSO.
Multi-SSO (SAML) IdP authentication flow

Access SNC Instance → Multi-SSO enabled? → No → Local DB

Yes → SAML SSO Cookie exist?

Yes → IdP used to create cookie

No → Auto-redirect IdP?

Yes → Auto-redirect IdP

No → Is IdP sso:xxx or federation:xxx?

Yes → Does user exist?

Yes → User Auto-provisioning IdP?

Yes → Auto-provisioning IdP

No → SSO:xxx → SSO associated IdP

No → Active default IdP?

Yes → Default IdP

No → Redirect fails. Contact your administrator.
If Multi-SSO is not enabled, authentication directs to a local DB.

**SAML SSO Cookie IdP**

If a SAML SSO cookie exists, the IdP which is specified with this cookie authenticates the user.

**Auto-redirect IdP**

If the auto-redirect IdP is enabled, this IdP authenticates the user.

**Federated IdP**

If the user browser is redirected to the external authorization (login_locate_sso.do) login screen, and the user exists in the user table with the IdP set in the **SSO Source** field as federation: xxx, then the federated IdP authenticates the user.

**Associated IdP**

If the user browser is redirected to the external authorization (login_locate_sso.do) login screen, and the user exists in the user table with the IdP set in the **SSO Source** field as sso: xxx, then the associated IdP authenticates the user.

**Auto-provisioning IdP**

If the user browser is redirected to the external authorization (login_locate_sso.do) login screen, and the user does not exist in the user table, but auto-provisioning is enabled, then the auto-provisioning IdP authenticates the user.

> **Note:** If there is more than one auto-provisioning IdP enabled, the user can choose the auto-provisioning IdP they can use.

**Default IdP**

If the user browser is redirected to the external authorization (login_locate_sso.do) login screen, and the user either:

- Does not exist in the user table, auto-provisioning is not enabled, and there is an active default IdP
- Exists in the user table, an IdP is not specified on the SSO source user or company record, and there is an active default IdP

then the default IdP authenticates the user.

Configure Multi-Provider SSO properties

Configure SSO properties and also add a property to the System Properties table to configure an IdP inclusion list.

Role required: admin

1. Navigate to **Multi-Provider SSO > Administration > Properties**.
2. Select the **Enable Multi-Provider SSO** check box. This selection adds the link Use external login to the login page.
3. To update the user table with the users in the IdP, select the **Enable Auto Importing** option.
4. To enable the debug messages to appear at the bottom of the content frame, select the **Enable debug logging for the Multi-Provider SSO integration** check box.

If enabled, the debug logging feature slows down performance and uses up disk space to generate logs.
5. In the property **The field on the user table that identifies a user accessing the User identification login page**, enter the field on the User table that contains the value the IdP uses to identify the user. The default value is **user_name**.

<table>
<thead>
<tr>
<th>Multiple Provider SSO Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Please edit your changes and press Save</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Customization Properties for Multiple Provider SSO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable multiple provider SSO</td>
</tr>
<tr>
<td>Enable Auto Importing of users from all identity providers into the user table</td>
</tr>
<tr>
<td>Enable debug logging for the multiple provider SSO integration</td>
</tr>
</tbody>
</table>

The field on the user table that identifies a user accessing the "User identification" login page. By default, it uses the 'user_name' field.

<table>
<thead>
<tr>
<th>user_name</th>
</tr>
</thead>
</table>

| Save |

| Multiple Provider SSO properties |

6. Click **Save**.

7. Instruct your users to click the **Use external login** link when they log in to the instance.

**Use OpenID Connect (OIDC) as a Single Sign-On (SSO) identity provider (IdP)**

OpenID Connect (OIDC) is an identity layer built on top of the OAuth protocol, which provides a modern and intuitive Single Sign-on (SSO) experience to you and your end users. OIDC also improves the login experience for mobile applications by enabling users to log in to ServiceNow applications using their social identity provider. For example, administrators can configure Single Sign-on with a third-party identity provider that supports OpenID Connect. Users then have the option to log in to your custom ServiceNow application using their identity provider credentials.

You can choose to use social identity providers like Google for your business-to-customer (B2C) users and enterprise identity providers like Okta, Microsoft Azure AD for your business-to-business users.

**Create an OpenID Connect (OIDD) configuration for Single Sign-On (SSO)**

You can create or update an OpenID Connect (OIDC) configuration using the Multi-Provider SSO plugin. If you have client ID, client secret, and well-known configuration URL of the identity provider, you can directly import the OIDC configuration for SSO. If you do not have the required information about the identity provider, you can manually configure OIDC for SSO. After completing the configuration, users can log in to ServiceNow applications using third-party social identity providers like Google, Okta.

- Register an OIDC application with your Identity Provider (IdP) and note the Client ID, Client Secret, and Well-known configuration URL.
- **Activate Multi-Provider SSO plugin**
- **Configure Multi-provider SSO properties**
- **Activate Approval with e-Signature plugin** to enable eSignature for the OIDC IdP.
• Role required: admin

1. Navigate to Multi-Provider SSO > Identity Providers.

2. Choose one of the following options:
   • To update an existing configuration, click an OIDC Identity Provider record.
   • To create a new configuration, click New > OpenID Connect.

3. For a new configuration, enter the OIDC configuration information in one of the following methods:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import OpenID Connect Well Known Configuration</td>
<td>If you have the well-known configuration URL along with your associated client credentials, you can directly import an OIDC configuration. <strong>Note:</strong> If you import the OIDC well-known configuration, all related fields are auto-populated.</td>
</tr>
<tr>
<td>Manually configure the OIDC Identity Provider form</td>
<td>If you do not have an existing OAuth OIDC Entity, close the Import OpenID Connect Well Known Configuration pop-up and manually fill the fields in the OIDC Identity Provider form.</td>
</tr>
</tbody>
</table>

**Import OpenID Connect Well Known Configuration fields**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name for the OIDC identity provider configuration.</td>
</tr>
<tr>
<td>Client ID</td>
<td>The client ID of the application registered in the third-party OIDC identity provider.</td>
</tr>
<tr>
<td>Client Secret</td>
<td>The client secret of the application registered in the third-party OIDC identity provider.</td>
</tr>
<tr>
<td>Well known Configuration URL</td>
<td>The URL that contains metadata about the third-party OIDC identity provider.</td>
</tr>
</tbody>
</table>

All required fields must be filled-in on the OIDC Identity Provider form.

Before you manually fill the OIDC Identity Provider form, ensure that you already have an OAuth Entity Profile for the OIDC IdP. If you do not have a OAuth Entity Profile, you can create it using the default External OIDC Provider templates, like Okta, Azure and others. The grant type of the OAuth Entity Profile must be authorization code. For more information, see Configure an OAuth OIDC provider on the Now Platform.

**Note:** You can use the templates of third-party identity providers, Auth0, Azure AD, Google, and Okta are available in the demo data of the Multiple Provider Single Sign-On Installer plugin.

**OIDC Identity Provider fields**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the OIDC identity provider record.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Active</td>
<td>Option to make the OIDC IdP configuration active.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This option can only be set to active after a successful test connection.</td>
</tr>
<tr>
<td>Default</td>
<td>Option to set the OIDC IdP configuration as default when there are more than one OIDC configurations.</td>
</tr>
<tr>
<td>Auto Redirect IdP</td>
<td>Option to enable auto redirection of the users to the login page of the identity provider. This field shows when the Set as Auto Redirect IdP option is set under the Related Links section.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you make a new Auto Redirect IdP configuration active, the glide_sso_id cookie automatically updates with the new Auto Redirect IdP. The glide.authenticate.sso.update.idp.cookie system property controls this feature.</td>
</tr>
<tr>
<td>OIDC Entity Profile</td>
<td>OAuth Entity Profile for the OIDC configuration.</td>
</tr>
<tr>
<td>ServiceNow Homepage</td>
<td>The URL of the login page used for authentication. This field is automatically set to your instance URL. The format of the URL is: https://&lt;yourinstance&gt;.service-now.com/navpage.do</td>
</tr>
<tr>
<td>External logout redirect</td>
<td>The URL where the integration redirects users after they log out. Typically, the portal which is used for SSO. This field is automatically set to external_logout_complete.do For example, https://&lt;yourinstance&gt;.service-now.com/external_logout_complete.do</td>
</tr>
<tr>
<td>Show as Login option</td>
<td>Option to display the OIDC IdP as a login option on the login page. The login option appears as the Login with &lt;Identity provider&gt; button.</td>
</tr>
<tr>
<td>SSO label</td>
<td>Label of the OIDC IdP displayed on the login page. This field appears only when Show as Login option is enabled.</td>
</tr>
<tr>
<td>Logo URL</td>
<td>Publicly available URL that contains logo of the OIDC IdP provider. This field appears only when Show as Login option is enabled.</td>
</tr>
</tbody>
</table>
4. Optional: User Provisioning tab

You can choose to enable automatic user provisioning during user login. When automatic user provisioning is enabled, a user record is automatically created in the ServiceNow instance if that user record does not exist.

**User Provisioning fields**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically provision users</td>
<td>Option to enable automatic user provisioning. This property creates a user in the instance User (sys_user) table when the user exits on IdP but does not exist in the User table.</td>
</tr>
<tr>
<td>Provision using</td>
<td>The data source to use to transform, an ID Token, User Info endpoint, or Both ID Token and User Info to a ServiceNow user. Use the Lookup list to select the pre-defined data source template, then open the record to configure the Transforms table mapping.</td>
</tr>
<tr>
<td>Provision data source</td>
<td>The ID token data source used for user provisioning.</td>
</tr>
<tr>
<td>User Info Datasource</td>
<td>The user info endpoint datasource used for user provisioning. This field is displayed when User Info or Both ID Token and User Info are selected for the Provision using field.</td>
</tr>
<tr>
<td>Update User on next login</td>
<td>Option to enable user update during the next login.</td>
</tr>
<tr>
<td>Update User Interval Time (Seconds)</td>
<td>Minimum time interval in seconds to update a user record between subsequent logins. This field is automatically set to 3,600 seconds. For example, after a user logs in, the user record will be updated after 3,600 seconds until the next login. This field is available only when the Update User on next login field is enabled.</td>
</tr>
<tr>
<td>User roles applied to provisioned users</td>
<td>List of roles applied to the newly provisioned users.</td>
</tr>
</tbody>
</table>

5. OIDC Entity tab

You can view and modify the OIDC client configuration and OIDC connect flow using the entity record.

6. OIDC Provider Configuration tab

You can view and modify the well-know configuration URL of the OIDC IdP or ID token claim validation.

7. Optional: Advanced tab

Scripts that are run during single sign-on and logout.

**Advanced fields**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Sign-On Script</td>
<td>The script that executes during Single Sign-On. This field is automatically set to MultiSSO_OIDC_custom.</td>
</tr>
<tr>
<td>Logout Script</td>
<td>The script that executes after user logs out. This field is automatically set to MultiSSO_OIDC_logout_custom.</td>
</tr>
</tbody>
</table>
8. Optional: eSignature Approval
You can configure eSignature for the OIDC IdP.

**Note:** The eSignature Approval tab appears only when you install the **Approval with e-Signature** plugin (com.glide.e_signature_approvals).

### eSignature Approval fields

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assertion Consumer URL for eSignature authentication</td>
<td>If you employ a customized method of handling the OIDC authentication for eSignature, you can set up your own consumer URL. For example, if you are using Multi-Provider SSO, you do not need to use this property. This format of the URL is https://&lt;yourinstance&gt;.service-now.com/consumer.do</td>
</tr>
<tr>
<td>Authentication Pop-up Dialog Width</td>
<td>Width of the authentication pop-up dialog. This field is automatically set to 800.</td>
</tr>
<tr>
<td>Authentication Pop-up Dialog Height</td>
<td>Height of the authentication pop-up dialog. This field is automatically set to 900.</td>
</tr>
</tbody>
</table>
9. Optional: Navigate to the login page of the instance to verify that IdP appears as a login option. The URL should be in the following format.

https://<yourinstance>/login_with_sso.do?glide_sso_id=sysId_IdP

**Note:** If you have enabled **Selected as Login Option**, you can go to the login URL of the instance.

---

Create a SAML 2.0 configuration using Multi-Provider SSO

You can create or update a SAML 2.0 SSO configuration from the Multi-Provider SSO feature.

Role required: admin

**Note:** New to the Jakarta release, you must validate your configuration by using the Test Connection functionality before you can activate your IdP configuration. You can still use the Update functionality to save your configuration data, but it is not an active configuration without a successful test connection.

1. Navigate to **Multi-Provider SSO > Identity Providers**.
2. Do one of the following options:
   - To update a configuration, click an SSO configuration record.
   - To create a new configuration, click **New > SAML**.
3. For a new configuration, enter the IdP information by one of the following methods:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using a metadata descriptor URL</td>
<td>Click the URL check box and enter the URL of the IdP that you are using.</td>
</tr>
<tr>
<td>Using metadata descriptor XML file</td>
<td>Click the XML check box and paste in the XML data generated from the IdP you are using.</td>
</tr>
<tr>
<td>Entering metadata manually</td>
<td>Close the popup window and manually enter the data in the property fields.</td>
</tr>
</tbody>
</table>

All required fields must be filled-in on the Identity Provider form.

**Multi-provider single sign-on fields**

<table>
<thead>
<tr>
<th>Property</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Yes</td>
<td>Enter the name for the SSO property record.</td>
</tr>
<tr>
<td>Active</td>
<td>Yes</td>
<td>Active should be set to true for the IdP to be used for authentication.</td>
</tr>
<tr>
<td>Default</td>
<td>No</td>
<td>The Auto Redirect IdP, formerly known as the Primary IdP, automatically redirects users to access the base instance URL. This property sets this IdP configuration as the default.</td>
</tr>
<tr>
<td>Auto Redirect IdP</td>
<td>No</td>
<td>Sets this IdP configuration as the Auto Redirect IdP.</td>
</tr>
<tr>
<td>Identity Provider URL</td>
<td>Yes</td>
<td>Enter the URL to your IdP. Each IdP URL must be unique.</td>
</tr>
</tbody>
</table>

Note: The option to set this property only comes after a successful test connection.

Note: If you make a new Auto Redirect IdP configuration active, the glide_sso_id cookie updates with the new Auto Redirect IdP. The glide.authenticate.sso.update.idp.cookie system property, automatically enabled, controls this feature.
<table>
<thead>
<tr>
<th>Property</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Provider's AuthnRequest</td>
<td>Yes</td>
<td>Enter the URL to the HTTP-Redirect binding obtained from the SingleSignOnService element.</td>
</tr>
<tr>
<td>Identity Provider's SingleLogoutRequest</td>
<td>No</td>
<td>Enter the URL obtained from the SingleLogoutService element.</td>
</tr>
<tr>
<td>ServiceNow Homepage</td>
<td>Yes</td>
<td>Enter the URL, including login page, of the instance for which the IdP authenticates. For example: <a href="https://yourinstance.service-now.com/navpage.do">https://yourinstance.service-now.com/navpage.do</a></td>
</tr>
<tr>
<td>Entity ID/Issuer</td>
<td>Yes</td>
<td>Enter the base URL, excluding login page, of the instance for which the IdP authenticates. For example: <a href="https://yourinstance.service-now.com/">https://yourinstance.service-now.com/</a></td>
</tr>
<tr>
<td>Audience URI</td>
<td>Yes</td>
<td>Enter the base URL, excluding login page, of the instance for which the IdP authenticates. For example: <a href="https://yourinstance.service-now.com/">https://yourinstance.service-now.com/</a></td>
</tr>
<tr>
<td>NameID Policy</td>
<td>Yes</td>
<td>Enter the value of the NameIDFormat element the integration uses.</td>
</tr>
<tr>
<td>External logout redirect</td>
<td>No</td>
<td>Enter the URL where the integration redirects users after they log out.</td>
</tr>
<tr>
<td>Failed Requirement Redirect</td>
<td>No</td>
<td>Enter the URL for redirecting failed authentication requests. Typically, the URL endpoint is an error page or logout page.</td>
</tr>
</tbody>
</table>
4. Optional: Encryption And Signing tab

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signing/Encryption Key Alias</td>
<td>Enter the alias of the key entry stored in SAML 2.0 SP Keystore.</td>
</tr>
<tr>
<td>Signing Key Password</td>
<td>Enter the password of the key entry stored in SAML 2.0 SP Keystore.</td>
</tr>
<tr>
<td>Encrypt Assertion</td>
<td>Select the check box to encrypt the assertion in the SAML response. The metadata generated for the IDP embeds the x509 certificate, which the IDP uses to encrypt the assertion in the SAML response that it generates.</td>
</tr>
<tr>
<td>Signing Signature Algorithm</td>
<td>Enter the URL that points to the SAML 2.0 Identity Provider AuthnRequest Consumer for eSignature Authentication.</td>
</tr>
<tr>
<td>Sign AuthnRequest</td>
<td>Select the check box to enable the IdP single-sign on service to receive a signed AuthnRequest.</td>
</tr>
<tr>
<td>Sign LogoutRequest</td>
<td>Select the check box to enable the IdP single-sign on service to receive a signed LogoutRequest.</td>
</tr>
</tbody>
</table>
5. Optional: User Provisioning tab

User Provisioning fields

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Provisioning User</td>
<td>Enable automatic user provisioning, which creates a user in the instance User table when the user exists on the IdP but does not exist in the User table.</td>
</tr>
<tr>
<td>Update User Record Upon Each Login</td>
<td>Updates user information in the instance User table with the information in the IdP each time the user logs in using SAML.</td>
</tr>
</tbody>
</table>

6. Optional: Advanced tab

Advanced fields

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Field</td>
<td>Enter the field on the User table that contains the value the IdP requires to identify the user.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>NameID Attribute</td>
<td>Leave this field blank unless you configure a new NameID policy. If you configure a new policy, the system requires the User table it must use to identify the user logging in. The system matches the NameID token to the name of that User table field here.</td>
</tr>
<tr>
<td>Create AuthnContextClass</td>
<td>Select the check box to specify a particular context class such as Password Protected Transport. If the check box is cleared, the IdP selects the most appropriate context class.</td>
</tr>
<tr>
<td>AuthnContextClassRef Method</td>
<td>Enter the URN of the login mechanism you want the IdP to use to authenticate users.</td>
</tr>
<tr>
<td>Force AuthnRequest</td>
<td>Select the check box to force AuthnRequests to occur.</td>
</tr>
<tr>
<td>Is Passive AuthnRequest</td>
<td>Select the check box if the AuthnRequest is passive.</td>
</tr>
<tr>
<td>Single Sign-On Script</td>
<td>Select the Single Sign-On script. The default is MultiSSO_SAML2_Update1.</td>
</tr>
<tr>
<td>Clock Skew</td>
<td>Enter the number of seconds between the two attributes that make up the SAMLResponse nonce. The default is 60. A valid SAMLResponse must fall between the notBefore and notOnOrAfter date-time values. See Sample SAML 2 Response with the SubjectConfirmation and SubjectConfirmationData Elements and Sample SAML 2 Response with the AudienceRestrictions and Audience Elements for a sample SAMLResponse message.</td>
</tr>
<tr>
<td>Protocol Binding for the IDP's SingleLogoutRequest</td>
<td>Enter one of the supported values listed in the Binding attribute from the SingleLogoutService element.</td>
</tr>
<tr>
<td>Metadata URL from which IDP properties are imported</td>
<td>The IdP properties import from this URL. If set, it enables the automatic import of SAML certificate from the IdP if the previous certificate has expired.</td>
</tr>
</tbody>
</table>

**Note:** If you upgrade from SAML2 Update 1 to Multi-Provider SSO or if you manually set up your SSO connection, the IdP Metadata URL does not automatically populate.

---

**X.509 certificates for SAML**

Store and activate the necessary IdP certificates for your SAML configuration.

The X.509 certificates are the IdP certificates that a SAML configuration uses. After you install a certificate, you can add as many certificates as necessary. When there are multiple certificates, the system uses the first active certificate that is found. If you set the URL for the Metadata URL from which IDP properties are imported field, the system automatically polls the IdP for a current, valid certificate when your certificate is no longer valid. It appends this certificate to your instance, and uses it for your active SAML configuration.

**Note:** Polling occurs if the IdP is accessible outside of your network.
Create and update identity providers

After you have configured the multi-provider SSO properties, you can update or create new SAML 2.0 Update 1 or digest token identity providers.

Role required: admin

1. Navigate to Multi-Provider SSO > Identity Providers.
2. To edit an identity provider record, click the record.
   - For digest token configurations, manually update the properties.
   - For SAML2 Update 1 configurations, automatically update the identity provider metadata with the Import Identity Provider Metadata related link or update the properties manually.
   - For OpenID Connect configurations, manually update the properties.
3. To create a new identity provider, click **New**.
   - For digest token configurations: Click **Digest SSO** and enter the digest properties for multi-provider single sign-on.
   - For SAML2 Update 1 configurations: Click **SAML2 Update 1** and import the identity provider metadata from a URL, as XML, or manually enter the identity provider information.
   - For OpenID Connect: Click **OpenID Connect** and enter client ID, client secret, and well known configuration URL.

4. To make the IdP the failover IdP that is used when the default IdP is not available, select the **Default** check box.
   - If you have SAML 2 Update 1 active and you upgrade to the Fuji release, the SAML 2 Update 1 IdP is selected as the default failover. No default failover IdP is selected for new instances or if you are upgrading from a release on which SAML 2 Update 1 is not active.

   **Note:** The metadata import process automatically creates a certificate record for the identity provider. Navigate to the **x509 Certificate** module to see the certificate.

   **Note:** Certificates for single-sign on should always be in PEM format to work with SAML certificates.

5. If E-Signature is active, configure the Identity Provider form and add the **Assertion Consumer URL for eSignature authentication** field.
   - In most cases, this URL is: `https://YOURINSTANCE.service-now.com/consumer.do`. However, if you employ a customized method of handling the SAML authentication for E-Signature, you can set up your own consumer URL. If you are only using SAML 2.0 Update 1 and not using Multi-Provider Single Sign-on, configure the assertion consumer URL with E-signature SAML properties.

Generate instance service provider (SP) metadata for SAML
   - As part of your SSO configuration, you can generate the instance SP metadata to provide to the IdP.

Role required: admin
The IdP needs the instance SP metadata to authenticate and forward requests.

1. Choose your installed SSO plugin:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-Provider SSO</td>
<td>Navigate to Multi-Provider SSO &gt; Identity Providers. Choose an IdP and click the Generate Metadata button. The integration automatically generates the instance's SP metadata from the system property settings.</td>
</tr>
<tr>
<td>SAML 2 SSO</td>
<td>Navigate to SAML 2 Single Sign-on &gt; Metadata. The integration automatically generates the instance's SP metadata from the system property settings.</td>
</tr>
</tbody>
</table>

2. Copy the SP metadata in the text box.

For example:

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
    entityID="https://yourinstance.service-now.com">
  <SPSSODescriptor AuthnRequestsSigned="false"
      WantAssertionsSigned="true"
      protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
                            Location="https://yourinstance.service-now.com/navpage.do" />
    <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
    <AssertionConsumerService isDefault="true" index="0"
     Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
     Location="https://yourinstance.service-now.com/navpage.do" />
    <AssertionConsumerService index="1"
     Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
     Location="https://yourinstance.service-now.com/consumer.do"/>
  </SPSSODescriptor>
</EntityDescriptor>
```

3. Provide the instance SP metadata to the IdP.
   For example, SSOCircle allows a user to provide the SP metadata online.

**Configure users for Multi-Provider SSO**

Administrators can configure Multi-Provider SSO for individual users or for all users who belong to a company. You cannot configure Multi-Provider SSO for groups.

Role required: admin

1. Navigate to Multi-Provider SSO > Identity Providers.
2. Right-click an identity provider record and select Copy sys_id.
3. Copy the data to your clipboard.
4. Navigate to a user record or a company record.
5. Configure the form and add the SSO Source field.
6. In the SSO Source field, enter one of the following:
   - SAML users: enter sso: followed by the sys_id of the identity provider's record.
   - SSO Federation users: enter federation: followed by the sys_id of the federation record.
7. Click Update.

**Testing IdP connections**

Testing the connection to an IdP validates the settings before enabling external authentication.

Role required: admin
The Jakarta release supports the test connection within a pop-up window. If your IdP does not work correctly with this option, you can turn off this default setting.

1. Navigate to **Multi-Provider SSO > Identity Providers**.
2. Select a defined IdP or click **New** to define a new IdP.
3. Optional: Configure an identity provider if setting up a new IdP.
4. Click **Test Connection**, enter login credentials for the IdP to check login.
   
   You cannot activate the IdP until you have a successful test connection. If the test fails, you can update to save your configuration information, but you cannot activate this configuration.

5. Verify results using the **SSO Test Results/Summary** or the **Testing SSO Logs** section to see log messages.
   
   If there are any errors, refer to the **Multi-SSO (SAML 2.0) errors and fixes**
6. Click **Cancel** when testing is complete.
SSO Login Test Results

- SAML Login response received
- SAML Assertion retrieved
- Signature Validated
- Certificate Validated
- Authorization/Condition Validated
- Certificate Issuer Validated
- Subject Confirmation Validated

SSO Logout Test Results

- SAML Logout response received
- SAML Logout Response 'inResponseTo' validated
- SAML Logout Response 'Status' validated

SSO Test Connection Summary

- Test connection is successful.

Click the "Activate" button to save and activate this configuration. Click the "Close" button to close this window and continue editing the SSO configuration.

```
02/21/17 17:10:01 (000) Issue Instant: 2017-02-22T01:10:01.000Z
02/21/17 17:10:01 (081) Session inResponseTo: SNcc17366dc961c8f8e6333eb974e22f9
02/21/17 17:10:01 (081) It is a logout response
02/21/17 17:10:01 (081) SAML LogoutResponse validated.
02/21/17 17:10:01 (082) request type : logoutResponse
02/21/17 17:10:01 (082) We will be redirecting user to the URL: /saml_test_conn_logout_completed.do?sysparm_nostack=true&sysparm_test_sso_id=7c623f133b121100027e5581b0e071355
02/21/17 17:10:01 (082) userToLogin: logout_success
```

Close  Activate
Common IdP connection errors
The following table describes some of the common IdP connection errors and their solutions.

### Troubleshooting IdP test connections

<table>
<thead>
<tr>
<th>Error messages</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Field validation failed. Invalid User Field <code>&lt;field name&gt;</code> is not a field on <code>sys_user</code> table.</td>
<td>Verify the contents of the User table field you selected matches the SAML NameID token.</td>
</tr>
<tr>
<td>Assertion issuer is invalid.</td>
<td>Verify <strong>Identity Provider URL</strong> contains a valid URL to your IdP. Each IdP URL must be unique.</td>
</tr>
<tr>
<td>AudienceRestriction validation failed.</td>
<td>Verify the <strong>Audience URI</strong> contains a valid URL to your instance.</td>
</tr>
<tr>
<td>Cannot logout of IdP's session.</td>
<td>Verify the <strong>SingleLogoutRequest URL</strong> contains a valid URL to your IdP's logout service.</td>
</tr>
<tr>
<td>Signature did not validate against the credential's key.</td>
<td>Verify the IdP has a valid certificate installed.</td>
</tr>
</tbody>
</table>

Multi-SSO (SAML 2.0) errors and fixes
A list of common errors and associated fixes for a Multi-SSO (SAML 2.0) setup and configuration.

### Errors during Multi-SSO (SAML 2.0) setup

<table>
<thead>
<tr>
<th>Error in instance logs</th>
<th>Test Connection Message</th>
<th>SAML property</th>
<th>Diagnosis</th>
<th>Fix</th>
</tr>
</thead>
<tbody>
<tr>
<td>NotAfter: <code>&lt;Thu Jun 05 22:57:44 PDT 2014&gt;</code>.</td>
<td>Ensure that the IDP x509 certificate is present, valid, and active.</td>
<td>N/A</td>
<td>The current certificate or the SAML assertion has expired.</td>
<td>• Sync the SNC clock with the SAML IdP server clock.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Update the SAML 2.0 certificate record.</td>
</tr>
<tr>
<td>• Unable to locate SAML 2.0 certificate.</td>
<td>Ensure that the IDP x509 certificate is present, valid, and active</td>
<td>The PEM-formatted string should be entered into the PEM Certificate field.</td>
<td>The SAML certificate does not exist. It might be inactive.</td>
<td>• Ensure that the correct PEM-formatted certificate is uploaded to the instance.</td>
</tr>
<tr>
<td>• Could not find a digital signature stored in the ServiceNow instance.</td>
<td>Ensure that the IDP x509 certificate is present, valid, and active</td>
<td>The PEM-formatted string should be entered into the PEM Certificate field.</td>
<td>The SAML certificate does not exist. It might be inactive.</td>
<td></td>
</tr>
<tr>
<td>Certificates do not match. Expect: <code>&lt;certStr&gt;</code>, actual: <code>&lt;inboundCert&gt;</code>.</td>
<td>Ensure that the IDP x509 certificate is present, valid, and active</td>
<td>N/A</td>
<td>The available certificate in SNC does not match the certificate in assertion. Causes include:</td>
<td>Confirm that the PEM-formatted string in the SAML 2.0 certificate record matches the X509 Certificate in the SAMLResponse for the user IdP.</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Error in instance logs</th>
<th>Test Connection Message</th>
<th>SAML property</th>
<th>Diagnosis</th>
<th>Fix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure to check the validity of the certificate.</td>
<td>Ensure that the IDP x509 certificate is present, valid, and active</td>
<td>N/A</td>
<td>The current certificate might have expired.</td>
<td>Update the SAML 2.0 certificate record.</td>
</tr>
<tr>
<td>Failure to validate signature profile.</td>
<td>Ensure that the IDP x509 certificate is present, valid, and active</td>
<td>N/A</td>
<td>The assertion might be signed with a different certificate.</td>
<td>Check if the IdP has the same certificate as the SNC instance.</td>
</tr>
<tr>
<td>InResponseTo attribute in SubjectConfirmationData mismatch. Expect: &lt;inResponseTo&gt;, actual: &lt;inResponseTo&gt;.</td>
<td>Subject confirmation validation failed.</td>
<td>N/A</td>
<td>This error appears if either of the following situations occurs:</td>
<td>The IdP admin should confirm that the expected SAMLResponse is being returned. This situation can be a load balancer or infrastructure issue.</td>
</tr>
<tr>
<td>SessionIndex value not found: &lt;message&gt;...</td>
<td>SessionIndex not valid.</td>
<td>N/A</td>
<td>The SessionIndex is required in the SNC instance. The IdP returns it in the SAML response to authenticate successfully.</td>
<td>The IdP admin should confirm that the SessionIndex is defined in the SAMLResponse.</td>
</tr>
<tr>
<td>No valid SubjectConfirmation found.</td>
<td>Subject confirmation validation failed.</td>
<td>N/A</td>
<td>Conditions could be missing due to an error on the IdP.</td>
<td>Review SAMLResponse to determine if Conditions are included in the SAMLResponse.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The StatusCode in the response would contain Responder instead of the expected Success.</td>
<td>The valid subject confirmation data could be expired or not for the right audience.</td>
</tr>
<tr>
<td>Error in instance logs</td>
<td>Test Connection Message</td>
<td>SAML property</td>
<td>Diagnosis</td>
<td>Fix</td>
</tr>
<tr>
<td>-----------------------------------------------------------</td>
<td>------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Assertion audience mismatch. Expect: &lt;propAudience&gt;, actual: &lt;audienceUri&gt;.  
  or  
  AudienceRestriction validation failed. No matching audience found. | Ensure that the 'Audience URI' field is set correctly.  
  The audience URI that accepts the SAML2 token. (Normally, it is your instance URI. For example: https://demo.service-now.com.) | The SNC instance configured audience URI must match the value in the IdP.  
  or  
  AudienceRestriction validation failed. No matching audience found. | Locate &lt;saml2:Audience&gt; in the SAMLResponse in the logs and verify that the value matches the one on the instance. |  |
| Assertion issuer is invalid. Expect: &lt;value on instance&gt;, actual: &lt;value returned by IdP&gt; | Assertion issuer is invalid.  
  The Identity Provider URL that issues the SAML2 security token with user info. | The IdP entity id (issuer) does not match the value defined in the SNC instance. |  
  or  
  AudienceRestriction validation failed. No matching audience found. | Check if IdP or SP is not configured properly.  
  Confirm that the SAML property (the Identity Provider URL that issues the SAML2 security token with user info) is set correctly. |
| Subject is valid in the future.  
  Now: &lt;now&gt;, NotBefore: &lt;notBefore&gt;  
  or  
  Subject is expired. Now: &lt;now&gt;, NotOnOrAfter: &lt;notOnOrAfter&gt; | Subject validation confirmation failed.  
  The number in seconds before notBefore constraint, or after notOnOrAfter constraint, to consider still valid. | The IdP clock is not synced with SP clock.  
  or  
  AudienceRestriction validation failed. No matching audience found. | Update the SAML property glide.authenticate.sso.saml2.clockskew to a larger value. The default is 180 seconds. Some cases require a setting of 300 or higher. You may also need to check the time on your IdP server. | |
| Assertion is valid in the future, now: &lt;now&gt;, notBefore: &lt;notBefore&gt;  
  or  
  Assertion is expired, now: &lt;now&gt;, notOnOrAfter: &lt;notOnOrAfter&gt; | Assertion is invalid.  
  The number in seconds before notBefore constraint, or after notOnOrAfter constraint, to consider still valid. | Idp clock is not synced with SP clock  
  or  
  AudienceRestriction validation failed. No matching audience found. | Update the SAML property to a larger value. Default of 60 seconds. Some cases require a setting of 300 or higher. You may also need to check the time on your IdP server. |  |
Common login and IdP errors

<table>
<thead>
<tr>
<th>Error or Symptom</th>
<th>Diagnosis</th>
<th>Fix</th>
</tr>
</thead>
</table>
| Login requests generate an infinite loop between the system and the IdP when High Security is active. | • Typically the URL endpoint is an error page or logout page.  
• The logout_redirect.do might create this loop when you define glide.security.url.whitelist without adding the IdP host name to the property value. | Set (or create) the system property glide.authenticate.failed_redirect to redirect failed authentication requests to this URL. |
| The token used to authenticate the user or the request is signed with the signature algorithm http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 which is not the expected signature algorithm http://www.w3.org/2000/09/xmldsig#rsa-sha1. | Check the Alert Context tab for event details.                                                | Navigate to the Advanced tab of the Relying Party Trust configuration dialog and verify that the algorithm is set to SHA-1 and not SHA-256. |

Troubleshoot script issues with SAML

You might encounter script issues if SAML is already active at the time you activate Multiple Single Sign-On and if you already customized the installation exits.

Role required: admin

1. Back up the modified installation exit SAML2SingleSignon_update1 and script include SAML2_update1.
2. Revert both the installation exit and script include to the version that is available with the baseline system.
3. Activate or upgrade the Integration - Multiple Provider Single Sign-On Installer plugin. The system upgrades SAML and all necessary files to SAML 2 Update 1.
4. Open the Multiple SSO properties page and select the Enable Multi-Provider SSO check box to enable it.
5. Put the SAML2SingleSignon_update1 installation exit changes into the baseline script include MultiSSO_SAML2_Update1 and the SAML2_update1 script include changes into the baseline SAML2_update1 script include.

Log in using Multi-Provider SSO

The recommended and most efficient method for users to log in using Multi-Provider SSO is to use a specifically configured URL.

Role required: admin

After multi-provider SSO is configured, you can send a URL to your users with the correct IdP in the parameter string. For example:

```
/login_with_sso.do?glide_sso_id=<sys_id of the sso configuration>
```

After a user successfully logs in to the IdP page, a cookie containing the IdP sys_id is added to the browser. The next time the user attempts to log in, the system redirects the user to log in to the IdP server, which automatically logs in to the instance.
If a URL parameter is not set or the browser cache has been cleared, users can also do the following:

1. Click the **Use external login** link on the login page.

   The external login page appears. Users can click **Use local login** to return to the standard login page.

2. Enter the value for the specified field on the user table that you configured in Multi-Provider SSO properties.

   The user is redirected to the IdP server, where they log in.

After users successfully log in to an IdP, they are automatically redirected to that IdP whenever they attempt to access the instance. To have a user access a different IdP, send the user a URL with the new IdP information in the parameter. The new IdP overwrites the old IdP in the cookie if the user successfully logs in. If the user does not log in successfully, the old IdP information is retained in the cookie.

**Allow users to choose the identity provider for login**

SSO federation support allows users to choose which IdP to log into.

Role required: admin

SSO federations aggregate metadata from multiple IdPs and service providers, including your instance. Federations then publish the metadata as an XML file, which includes information like IdP names and IdP certificates. Administrators can then instruct the instance to read the XML file and automatically populate the SSO Properties table with all the necessary IdP information.

1. Navigate to **Multi-Provider SSO > SSO Federation**.
2. Click **New**.
3. Fill in the fields, as appropriate (see table).
4. Click **Submit**.
5. After you configure a federation, enable the Refresh SSO Metadata scheduled job, and then configure the users who you want to access the federation IdPs. Use the sys_ID of the federation record you just created.

The instance populates the SSO properties table with the IdP information. When users who are configured to use the federation log in, they are redirected to the discovery service URL you configured. Then they select the IdP and provide the necessary credentials. Alternatively, you can send users a URL with the IdP in the parameter.

### Allowing users to choose the identity provider for login

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a descriptive name for the federation.</td>
</tr>
<tr>
<td>Active</td>
<td>Select the check box to enable the instance to pull the XML file from the federation.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the type of authentication this federation supports.</td>
</tr>
<tr>
<td>Discovery Service URL</td>
<td>Enter the URL of the discovery service for this federation. This is the site where users are directed to select an IdP and log in.</td>
</tr>
<tr>
<td>Meta Data URL</td>
<td>Enter the URL of the XML file that holds the federation metadata.</td>
</tr>
<tr>
<td>x509 Certificate</td>
<td>Select the federation certificate.</td>
</tr>
<tr>
<td>Domain</td>
<td>Select the domain that the data will belong to.</td>
</tr>
</tbody>
</table>

**Note:** The InCommon federated identity management IdP is preconfigured.

**Use Service Portal with Multi-Provider SSO to redirect a URL**

Service Portal uses a combination of system properties and script includes to determine how the system handles URL redirects for users logging in to the portal.

Role required: admin
If you are using the system property to automatically redirect to your primary Identity Provider (IdP), then Service Portal automatically redirects to that IdP. If you have multiple IdPs, Service Portal shows a link on the login page to **Use external login**.

1. Configure the Service Portal login page
2. Redirect to Service Portal after login

**Use Multi-Provider SSO to set up an SSO approval for a SAML 2.0 authentication**

An SSO approval with e-signature requires configuration on the SAML IdP and the ServiceNow instance.

The SAML IdP must support and honor the forceAuthn attribute in SAML assertion requests. E-signature does not function without this IdP setting. Set up an approval with e-signature using credentials from a SAML 2.0 authentication.

1. Activate or upgrade to SAML 2.0 with the Integration - Multiple Provider Single Sign-On Installer plugin.
2. Activate the Approval with E-Signature plugin.
3. Navigate to Multi-Provider SSO > Identity Providers and verify your 2.0 SAML IdP configuration.
   
   Advanced tab shows the **Force AuthnRequest** attribute checked.

   Your SAML 2.0 IdP must support the **Force AuthnRequest** attribute, or e-signature is not supported.

4. On the eSignature Approval tab, enter the following e-signature SAML properties:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Assertion Consumer URL for eSignature authentication</strong></td>
<td>This property defaults to the appropriate URL. To configure this property, click the lock icon to make this field editable. After edits, click the icon to lock the field.</td>
</tr>
<tr>
<td><strong>Assertion Consumer Index for eSignature authentication</strong></td>
<td>If your Service Provider has more than one URL set for the AssertionConsumerURL, you can set the index to use for eSignature, starting with index 1 or more.</td>
</tr>
<tr>
<td><strong>AuthnRequest URL for eSignature Authentication</strong></td>
<td>You can enter the URL that points to the SAML 2.0 IdP AuthnRequest URL for eSignature authentication. If the URL is the same as the Assertion Consumer URL, you can leave this setting blank.</td>
</tr>
<tr>
<td><strong>Authentication Pop-up Dialog Width</strong></td>
<td>When a user approves a request using eSignature, a dialog opens and a user can enter credentials. This setting controls the width of that dialog box. The default is 500.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Authentication Pop-up Dialog Height</td>
<td>When a user approves a request using eSignature, a dialog opens and a user can enter credentials. This setting controls the height of that dialog box. The default is 300.</td>
</tr>
</tbody>
</table>

5. Click the **Generate Metadata** button underneath the tabs to regenerate the service provider metadata. Copy this data and update it on the SAML IdP.

**Activate Approval with e-Signature plugin**

The Approval with e-Signature plugin (com.glide.e_signature_approvals) allows users to approve requests by re-entering their login credentials.

Role required: admin

1. Navigate to **System Applications > All Available Applications > All**.
2. Find the plugin using the filter criteria and search bar.

You can search for the plugin by its name or ID. If you cannot find a plugin, you might have to request it from ServiceNow personnel. For more information, see Request a plugin.
3. Click **Install**, and then in the Activate Plugin dialog box, click **Activate**.

**Note:** When domain separation and delegated admin are enabled in an instance, the administrative user must be in the **global** domain. Otherwise, the following error appears: Application installation is unavailable because another operation is running: Plugin Activation for <plugin name>.

**Changes to SAML 2.0 and digest token configuration**

Multiple provider single sign-on allows administrators to configure SAML 2.0 Update 1 and digest token as authentication methods.

Multiple provider single sign-on should be activated before you configure your SAML 2.0 Update 1 and digest token properties. After you request and activate multi-provider SSO, you must then set it up. After setting up multi-provider
SSO, you can create or update the SAML 2.0 Update 1 and digest token configurations. You can use either or both authentication solutions with multi-provider SSO.

**Note:** The Integration - Multiple Provider Single Sign-On Installer plugin removes the SAML application from the navigator. The necessary SAML settings are migrated to the Multi-Provider SSO application into the SAML2 Migrated table. You can still modify items like the x509 certificate, IdP details, and so on through the Multi-Provider SSO application.

### LDAP integration

An LDAP integration allows your instance to use your existing LDAP server as the master source of user data.

Administrators integrate with a Lightweight Directory Access Protocol (LDAP) directory to streamline the user login process and to automate administrative tasks such as creating users and assigning them roles. An LDAP integration allows the system to use your existing LDAP server as the primary source of user data. Typically, an LDAP integration is also part of a single sign-on implementation.

The integration uses the LDAP service account credentials to retrieve the user distinguished name (DN) from the LDAP server. Given the DN value for the user, the integration then rebinds with LDAP with the user's DN and password. The password that the user enters is contained entirely in the HTTPS session. The integration never stores LDAP passwords.

The integration uses a read-only connection that never writes to the LDAP directory. The integration only queries for information, and then updates its internal database accordingly.
Example LDAP Integration - User Import

**Note:** For detailed information about setting up the integration, see LDAP integration setup.

**Note:** If your instance is using an LDAP integration and the Active Directory settings require users to reset their password upon login, your users will not be able to log in the instance. The instance cannot change any user’s active directory password.

**Features of LDAP integration**

LDAP integration features include the following.

**Scheduled LDAP refresh**

A scheduled scan of your LDAP server is usually run once a night. It queries all applicable user records' attributes and compares them with the account on our servers. If there is a difference, we modify our user record with the changed attribute. The load placed upon the LDAP server during the refresh depends on how many records are queried, and the number of attributes being compared. We recommend scheduling the refresh during off-peak hours.
A large refresh operation can affect other scheduled operations, such as running reports, and should be planned to minimize any conflicts.

**LDAP listener**

LDAP listener is our version of a persistent query (or persistent search). We issue a standing query for changes made to your LDAP server, and constantly listen for a response. Assuming your server supports a persistent search, any changes made to any of your applicable LDAP accounts are returned to the LDAP listener and sent to your instance within approximately 10 seconds. This is an extremely useful tool, allowing us to have a nearly real-time copy of your users' account details, without having to wait for the next scheduled refresh.

**On-demand LDAP login**

After an LDAP integration is established, the instance can allow new users to log in to the system even if they do not yet have an account on the instance. When a new user attempts to log in to the instance, the integration checks to see if this user has an account in the instance. If the integration does not find an existing user account, it automatically queries the LDAP server for the username that was entered. If a matching LDAP account is found, the integration tries to authenticate with the password the user entered. If the password is valid, the instance creates an account for the user, populates the account with all applicable LDAP information, and logs the user in to the instance.

On-demand login uses the LDAP User Import transform map. For more information on transform map requirements, see [LDAP transform maps](#).

**LDAP data population**

- **Note:** Functionality described in this integration is not available by default. This integration involves post-deployment customization performed by an experienced administrator or by ServiceNow professional services consultants.

An integration to the LDAP servers allows you to quickly and easily populate the instance's database with user records from the existing LDAP database. To prevent data inconsistencies, you can create, ignore, or skip incoming LDAP records.

You can also limit the data the integration imports by specifying LDAP attributes, thereby importing only the data that you want to expose to an instance. Typically, the LDAP attributes you specify become part of the integration transform map. If you do not specify any LDAP attributes, the integration imports all available object attributes from the LDAP server. The instance stores imported LDAP data in temporary import set tables, so the more attributes you import, the longer the import time. For more information, see [Specify LDAP attributes](#).

**LDAP authentication**

Use LDAP authentication to access using LDAP credentials.

When a user enters network credentials in the login page:

1. The instance passes the credentials to an LDAP server to find the instance.
2. With RDNs, it validates the user's DN string. It validates only if at least one of the LDAP OU configurations with `table=sys_user` has an RDN configured.
3. The LDAP server responds with an authorized or unauthorized message that the system uses to determine whether access should be granted.

By authenticating against your LDAP server, users access the platform with the same credentials that they use for other internal resources on your network domain. Also, you can reuse any existing password and security policies that are already in place. For example, the LDAP server may already have account lockout and password expiration policies.

When you enable LDAP, the system updates user records with these fields.
**LDAP user record updates**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Identifies whether or not LDAP is used to validate a user. If the source starts with ldap, then the user is validated via LDAP. If the source does not start with ldap, then the password on the user record is used to validate the user upon login.</td>
</tr>
<tr>
<td>LDAP Server</td>
<td>Identifies which LDAP server authenticates the user when there are multiple LDAP servers.</td>
</tr>
</tbody>
</table>

**Note:** The system does not support LDAP password authentication through a MID Server. An instance must be able to directly connect with an LDAP server to support password authentication.

**Understanding LDAP integration**

An LDAP integration allows your instance to use your existing LDAP server as the primary source of user data.

**LDAP integration prerequisites**

- The directory services server must be LDAP v3 compliant
- Inbound network access through the firewall must be allowed (to the LDAP server)
- External IP or Name of the LDAP server
- User credentials with read-only access
- For LDAPS, a PKI certificate

**LDAP integration timing**

LDAP integrations are usually done before the instance Go Live, but can be integrated at any time.

**LDAP server data integrity**

Some users are concerned about a third party (the instance in this case) making changes (writing) to your LDAP server. In an LDAP integration, your instance does not write to the internal LDAP directory. The instance queries for information, and updates its database accordingly.

No changes are made to the internal LDAP server by the instance. The service account is read only.

Most changes (including additions) to your LDAP server are available to the instance within seconds, depending on how many components of the full LDAP integration are in place.

To keep LDAP records synchronized, schedule a periodic scan of the LDAP server to pick up changes.

The instance does not synchronize department records. Users and group memberships are kept up-to-date by the LDAP Listener mechanism and a daily full LDAP Browse, but the instance does not delete any of these entries once they disappear from LDAP.

If an entry were to be deleted, the entire history would also get deleted, and any references to it would be cleared or deleted. Configuration Items (CIs), SLA Agreements, Software Licenses, Purchase Orders, and Service Catalog Entries all have a reference to Department, and if Department is deleted, then those references get cleared. There are
many references to Users, and so deleting a user would lose all history of what that user did. Currently, the decision to
delete or not to delete is made by our customers.

Security

The connection is made from a single machine using a fixed IP address through a specific port on your firewall.
Authentication is done with a read-only LDAP account of your choosing. You can use standard LDAP, or load the
public side of an SSL certificate installed on your directory, in which case we can use LDAPS. To add another layer
of security, we also offer the option of a point-to-point IPSEC VPN tunnel. Speak to your account manager for details
and pricing.

Secure LDAP connections

<table>
<thead>
<tr>
<th>Connection</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MID Server</td>
<td>To shield your LDAP server from external network traffic, install a MID Server on the local network and configure the system to communicate with the MID Server over a secure channel.</td>
</tr>
<tr>
<td>LDAPS</td>
<td>To establish an encrypted LDAPS connection, load the public side of your LDAP server's SSL certificate. The integration uses the certificate to encrypt all communication between the LDAP server and the instance.</td>
</tr>
<tr>
<td>VPN</td>
<td>To secure the LDAP server with an encrypted point-to-point IPSEC VPN tunnel, speak to your account manager for details and pricing.</td>
</tr>
</tbody>
</table>

Another security aspect to consider is the data shared in an LDAP integration. To limit the data exposed to your
instance, specify attributes in your transform map. For more information, see LDAP transform maps.

Importing LDAP data to the instance

It is recommended that attributes are defined to import only required data. Defined attributes get mapped into the
instance user database.

We cannot answer the question of which specific attributes are needed because this is determined by the scope of the project and business requirements.

Supported types of LDAP servers

The instance has successfully integrated with Microsoft Active Directory, Novell, Domino (Lotus Notes), and Open LDAP. We use JNDI to interface with the LDAP Server. As long as your LDAP server is LDAP v3 compliant, the integration is successful.

LDAP single-sign-on

Along with the data population functionality provided with the LDAP import, you can use the External Authentication functionality supported by the application to prevent your users from needing to sign on each time.
Multiple LDAP domains

The recommended method for handling multiple domains is to create a separate LDAP server record for each domain. Each LDAP server record must point to a domain controller for that domain. This means the local network must allow connections to each of the domain controllers.

After expanding to more than one network domain, it is critical that you identify unique LDAP attributes for the application usernames and import coalesce values. A common unique coalesce attribute for Active Directory is `objectSid`. Unique usernames may vary based on the LDAP data design. Common attributes are `email` or `userPrincipalName`.

Handling query limits

By default, Active Directory 2000/2003 has an LDAP query limit (`maxPageSize`) of 1000 objects to prevent excessive loads and denial of service attacks. We have two methods of dealing with this limit.

The default method is to break up the query to return less than 1000 objects at a time. For example, query only for object starting with the letter 'a', then query for 'b' objects. The more efficient method for large environments is to enable paging. Paging is supported by default on all Microsoft Active Directory servers. It automatically splits the results into multiple result sets, so we don't have to split up the query into multiple requests.

LDAP query type

If an LDAP password is supplied then a "Simple Bind" is performed. If no LDAP password is supplied then "none" is used, in which case the LDAP server must allow anonymous login.

LDAP authentication

We use provided service account credentials for LDAP to retrieve the user DN from the LDAP server. Given the DN value for the user, we then rebind with LDAP given the users DN and the provided password.

Password storage

The password that the user enters is contained entirely in their HTTPS session. We do not store that password anywhere.

Setting up LDAP authentication

These fields on the user record pertain to LDAP:

- **Source**: The Source field identifies whether or not a user is validated using LDAP. If the source field starts with "ldap", then the user is validated via LDAP. If the Source field does not start with "ldap", then the password on the user record is used to validate the user upon login.
- **LDAP Server**: The instance supports multiple LDAP servers, so the LDAP Server field determines which server should be used to authenticate the user.

LDAP integration requirements

Review the requirements for LDAP integration, which include a PKI certificate an LDAP compliant directory services server.

LDAP integration requires:
• An LDAP v3 compliant directory services server
  • Allows inbound network access through the firewall (to the LDAP server)
  • (Optional) Accepts anonymous login
  • (Optional) Supports paging for large LDAP queries

• The external IP address or fully-qualified domain name of the LDAP server. You can also use a MID server.
• A read-only LDAP account of your choosing
• For multiple domains, network access for each domain controller
• For LDAPS, a PKI certificate
• For LDAP listener, a Microsoft Active Directory server that supports persistent queries (ADNotify)

Supported LDAP servers

Using JNDI to interface with the LDAP server, the instance has successfully integrated with the following servers:
• Microsoft Active Directory
• Novell
• Domino (Lotus Notes)
• Open LDAP

LDAP query limits

By default, Active Directory 2000/2003 has an LDAP query limit (maxPageSize) of 1000 objects to prevent excessive loads and denial of service attacks. The system has two methods of dealing with this limit.
• The default method is to break up the query to return fewer than 1000 objects at a time. For example, query only for objects starting with the letter a, then query for b objects.
• The more efficient method for large environments is to enable paging, which is supported by default on all Microsoft Active Directory servers. Paging automatically splits the results into multiple result sets so the integration does not have to split up the query into multiple requests.

LDAP integration setup

Administrators can enable LDAP integration to allow sign-on of users from their company LDAP directory.

LDAP typically uses one of these types of communication channels.
## LDAP communication channels

<table>
<thead>
<tr>
<th>Connection</th>
<th>Description</th>
<th>LDAP import support?</th>
<th>LDAP authentication support?</th>
</tr>
</thead>
<tbody>
<tr>
<td>MID Server connection</td>
<td>Communicates over HTTP on port 80 by default. This communication channel does not require a certificate. The connection between the MID Server and the instance is over HTTPS (port 443). You can use the MID Server to import data over LDAP, but you cannot use the MID Server for LDAP authentication. Proceed to Define the LDAP Server.</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Standard LDAP integration</td>
<td>Communicates over TCP on port 389 by default. This communication channel does not require a certificate. Proceed to Define the LDAP Server.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SSL-encrypted LDAP integration (LDAPS)</td>
<td>Communicates over TCP on port 636 by default, This communication channel requires a certificate. Proceed to Install the LDAP X.509 SSL certificate to obtain and upload the certificate.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>VPN connection</td>
<td>Communicates over an IPSEC tunnel. Purchase or create an IPSEC tunnel on your local network. Proceed to Define the LDAP Server.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

If using a MID Server, the MID Server connects to the instance and the MID Server also connects to the LDAP server. In both cases, the MID Server initiates the connection:

1. First, the MID Server connects to the LDAP server via LDAP on Port 389.
2. Then, the MID Server initiates an HTTPS encrypted connection to the instance on Port 443 to push the data to the instance.

For more information about VPNs, Mid Servers, and LDAP, see You Don't Need A VPN Part II on the community.

### Install the LDAP X.509 SSL certificate
You can install an X.509 certificate for your LDAP integration.

Role required: admin

1. Purchase or generate an SSL certificate on your LDAP server.
3. Fill in the form fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The certificate name.</td>
</tr>
<tr>
<td>Expiration notification</td>
<td>Select this option to send a notification to the users selected in the Notify on expiration field. By default, this is enabled.</td>
</tr>
<tr>
<td>Notify on expiration</td>
<td>Select the users to revive the notification regarding certificate expiration. If no users are selected, the logged in user is added by default, along with the last two logged in users with the administrator role.</td>
</tr>
<tr>
<td>Warn in days to expire</td>
<td>The number of days before expiration that the instance send the notification. Enter a value of at least 20. Instances upgraded to Istanbul and later releases have this value set to 20 unless a greater value is specified.</td>
</tr>
<tr>
<td>Active</td>
<td>A check box to indicate that this certificate is active.</td>
</tr>
<tr>
<td>Format</td>
<td>The format of the certificate.</td>
</tr>
<tr>
<td>Type</td>
<td>The certificate container. The instance recognizes certificates from trust stores, Java keystore, and PKCS#12 keystores.</td>
</tr>
<tr>
<td>Valid from</td>
<td>The instance automatically adds the certificate valid from date to this field. Attach the certificate to the X.509 certificate record to populate this field.</td>
</tr>
<tr>
<td>Expires</td>
<td>The instance automatically adds the certificate expiration date to this field. Attach the certificate to the X.509 certificate record to populate this field.</td>
</tr>
<tr>
<td>Expires in days</td>
<td>The calculated number of days to expiration.</td>
</tr>
<tr>
<td>Short description</td>
<td>A description for the certificate.</td>
</tr>
<tr>
<td>Issuer</td>
<td>The instance automatically adds the certificate issuer to this field. Attach the certificate to the X.509 certificate record to populate this field.</td>
</tr>
<tr>
<td>Subject</td>
<td>The instance automatically adds the certificate subject to this field. Attach the certificate to the X.509 certificate record to populate this field.</td>
</tr>
<tr>
<td>PEM Certificate</td>
<td>Enter the value of the X509 certificate.</td>
</tr>
</tbody>
</table>

**Note:** The integration does not currently sign the certificate in communications between the instance and the IdP.

4. Click **Save**.

Click **Validate Stores/Certificates** to test the trust store and certificate.

**Define an LDAP server**

Create a new LDAP server record in the instance.

Role required: admin

1. Navigate to **System LDAP > Create New Server**.
2. Fill in the form fields.

In the **Server URL** field, the valid URLs of all servers appear separated by a space. Servers are first ordered by operational status, with servers that are **Up** listed first, then ordered by the **Order** value that you specify. The first server listed is the primary LDAP server. The others are redundant servers.

**Note:** There is a slight delay between the change in the actual operational status and the display.

Alternatively, you can add a redundant LDAP server by navigating to an existing LDAP server record and inserting a row in the LDAP Server URLs embedded list.
3. Click **Submit**.

**Note:** You can also modify an existing LDAP server record by navigating to **System LDAP > LDAP Servers** and making the needed changes.

4. Make changes to the fields as necessary.

### LDAP server form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the server.</td>
</tr>
<tr>
<td>Active</td>
<td>Select this check box if the server is active.</td>
</tr>
<tr>
<td>LDAP Server URLs</td>
<td>Enter the URLs of the primary and backup LDAP servers. Servers are first ordered by operational status, with servers that are Up listed first, then ordered by the Order value that you specify. The first server listed is the primary LDAP server. The others are redundant servers.</td>
</tr>
<tr>
<td>Server URL</td>
<td>Enter the URL of the server. Configure the form to add this field if necessary. It is a calculated read-only field that shows the list of LDAP servers that you can also see in the <strong>LDAP Server URLs</strong> field, separated by a space, and ordered by operational status and the order values of the URLs.</td>
</tr>
</tbody>
</table>
| Login distinguished name | Enter the distinguished name (DN) of the user authenticating the LDAP connection. To access an LDAP directory server, the username must be in the full distinguished name format:  
  ```
  servicenow@service-now.com
  ``` |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login password</td>
<td>Enter the server’s password.</td>
</tr>
<tr>
<td>Starting search directory</td>
<td>Enter the relative distinguished name (RDN) of the default search directory. All queries to this LDAP server will start from this RDN.</td>
</tr>
<tr>
<td>MID Server</td>
<td>Select the MID Server you want to use to connect to the LDAP server. Using a MID Server to establish an LDAP connection prevents you from having to expose the LDAP server to external network traffic. It also eliminates the need to establish a VPN tunnel between your LDAP server and ServiceNow data centers.</td>
</tr>
<tr>
<td>Connect timeout</td>
<td>If a MID Server is configured, the connection times out after 10 seconds, regardless of this setting. This setting is hard-coded and cannot be altered.</td>
</tr>
<tr>
<td>Read timeout</td>
<td>Specify the number of seconds the integration has to read LDAP data. The integration stops reading LDAP data after the connection exceeds the read timeout. If you enable an SSL connection, you can also set a read timeout value with the <code>com.glide.ssl.read.timeout</code> system property. If you enter timeout values for both this field and the system property, the lowest timeout value takes precedence.</td>
</tr>
<tr>
<td>SSL</td>
<td>Select this check box to require the LDAP server to make an SSL-encrypted connection. If you selected a MID Server, this field is not available. If you use an LDAPS integration and the default SSL port is 636, no further configuration is necessary; SSL is automatically enabled. If the LDAPS integration uses another SSL port, define the alternate SSL connection properties.</td>
</tr>
</tbody>
</table>

**Note:**
- The MID Server user must have the `user_admin` role in order to be able to read LDAP server configuration records.
- The following are not available with the MID Server:
  - LDAP authentication
  - SSL connection

**Note:**
Be sure a network administrator configures the local firewall to allow the application server to access the LDAP server. If the LDAP server is located within an internal network, the firewall forwards (or NATs) the application server’s IP address through the firewall on the correct port.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Listener</td>
<td>Select this check box to enable the integration to periodically poll Microsoft Active Directory servers or LDAP servers that support persistent search request control. Additionally, if you selected a MID Server, the listener functionality is available for that MID Server. See Enable an LDAP listener and set system properties for more information.</td>
</tr>
<tr>
<td>Listen interval (timeout value)</td>
<td>Specify the listener timeout value in the number of minutes that the integration listens for LDAP data with every connection. The integration stops listening for LDAP data after the connection exceeds the listen interval.</td>
</tr>
<tr>
<td>Paging</td>
<td>Select this check box to have the LDAP server split up LDAP attribute data into multiple result sets rather than submit multiple queries.</td>
</tr>
</tbody>
</table>

**Note:** If you provide an LDAP password, the integration performs a Simple Bind operation. If you do not provide an LDAP password, the LDAP server must allow anonymous login or the integration cannot bind to the LDAP server.

When an LDAP Server record is set to active, the system automatically tests every connection to validate it.

Validations include:
- The LDAP server is accessible at the provided URL and port
- The LDAP server URL is properly formatted
- The login credentials are valid

Starting with the Fuji release, the system displays colored dots next to each server URL:

**LDAP server connection icons**

<table>
<thead>
<tr>
<th>Color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>The server if active and operational.</td>
</tr>
<tr>
<td>Gray</td>
<td>The server is neither active nor operational.</td>
</tr>
<tr>
<td>Red</td>
<td>The server is active but not operational.</td>
</tr>
</tbody>
</table>
LDAP server connection status
**Enable an LDAP listener and set system properties**

Enabling a listener is optional. If enabled, a listener notifies the system to process LDAP records soon after there is an update on the LDAP server.

Role required: admin

A **listener** is a dedicated process that periodically searches for changes on the LDAP server.

The listener can be deployed on a Microsoft Active Directory server that supports persistent queries (ADNotify), or on an LDAP server that supports persistent search request control (with OID 2.16.840.1.113730.3.4.3).

If the LDAP server supports a persistent search, the LDAP listener recognizes any user and group changes made to any of the applicable LDAP accounts and forwards them to your instance within approximately 10 seconds. This allows the instance to have a nearly real-time copy of your users' account details without having to wait for the next scheduled refresh. The LDAP listener can only synchronize objects that map to the User [sys_users] and Group [sys_user_group] tables.

**Note:** If a user is added via the listener, but the user does not meet the requirements as defined by the OU filter, then the instance ignores the record on the LDAP server. If it meets the criteria, the user is added to the instance.

To enable a listener:

1. Navigate to **System LDAP > LDAP Servers**.
2. Select the LDAP server to configure.
3. Select the **Listener** check box.
4. Click **Update**.

**Note:**

The system only imports user records that match the LDAP OU filter. Incoming user records that do not meet the filter requirements are flagged as invalid and ignored by the import. Administrators can enable verbose LDAP logging to determine if incoming records are not matching the LDAP OU filter.
5. Optionally navigate to the sys_properties table and set LDAP listener system properties.

### LDAP listener properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.ldap.listener.use_background_transaction</td>
<td>When true, the LDAP listener is started as a background transaction. By running the LDAP listener as a background transaction, the quota rule LDAP Listener Start/Stop Transaction can cancel the transaction after the maximum duration is reached, 5 minutes by default. This behavior prevents an LDAP listener from waiting indefinitely.</td>
<td>This property applies only to LDAP connections that do not use a MID Server. Use glide.ldap.listener.mid.use_background_transaction to control the behavior of LDAP connections that go through a MID Server.</td>
</tr>
<tr>
<td>glide.ldap.listener.mid.use_background_transaction</td>
<td>When true, the LDAP listener is started as a background transaction. By running the LDAP listener as a background transaction, the quota rule LDAP Listener Start/Stop MID Transaction can cancel the transaction after the maximum duration is reached, 5 minutes by default. This behavior prevents an LDAP listener from waiting indefinitely.</td>
<td>This property applies only to LDAP connections that use a MID Server. Use glide.ldap.listener.use_background_transaction to control the behavior of LDAP connections that do not go through a MID Server.</td>
</tr>
<tr>
<td>glide.ldap.listener.mid.one_listener</td>
<td>When true, only a single ECC queue message is created to start or stop the LDAP listener through a MID Server. When false, multiple ECC queue messages can be created, leading to the creation of multiple threads to start or stop the LDAP listener.</td>
<td></td>
</tr>
</tbody>
</table>
Specify LDAP attributes

Specify the attributes included in LDAP server queries using the LDAP server Attributes field. This can enhance performance as well as security.

Role required: admin

By default, the system loads all of the attributes for each object that it has permission to read from your LDAP server. Using the Attributes field, you can specify and thereby limit the attributes the LDAP query returns. Using this approach for large LDAP imports can greatly improve the speed of those imports.

Explicitly define attributes where possible. If there is information that you do not want exposed to the instance, exclude the attribute.

If you do not specify LDAP server attributes, user transactions may freeze for extended periods of time when new attributes are added to an LDAP server object because the system will be busy loading data from the new attributes.

Note: To use the manager lookup scripts described in Select or Create a Transform Map for LDAP Data, specify manager and dn (distinguished name) in the Attributes field. Neither attribute is required to be a part of a transform map.
Test an LDAP connection
The instance tests the connection automatically every time a user opens the LDAP Server form. Alternatively, you can manually test the connection to the LDAP server from the LDAP server form.

Role required: admin

By default, error messages appear on the LDAP server form if there are any issues connecting to the LDAP server.

**Note:** Employees can also verify connectivity between the instance and the LDAP server. Contact Technical Support for assistance verifying LDAP connectivity.

To manually test a connection:

1. Navigate to System LDAP > LDAP Servers.
2. Select the LDAP server to test.
3. Under Related Links, click Test connection.
4. Under Related Links, click Browse to verify that the appropriate LDAP directory structure is visible to the system.
5. (Optional) If the connection was successful, click **Browse** to view the source LDAP directory structure that is visible to the instance.

   ![Note: The Filter and RDN fields on the left of the Browse window are ignored when you use the search field on the right.]

The instance changes the operational status of LDAP servers depending on the result of the connection test.

- If your instance establishes a connection to a server that has a **Operational Status** value of **down**, the **Operational Status** value is automatically changed to **up**. This functionality is supported for both automatic and manual connection tests.
- If a connection cannot be established to a server that has a **Operational Status** value of **up**, the **Operational Status** value is automatically changed to **down**. This functionality is supported for automatic connection tests only, not manual tests.

**Define LDAP organizational units**
An organizational unit (OU) definition specifies the LDAP source directories available to the integration.

Role required: admin

OU definitions can contain locations, people, or user groups. Every LDAP server definition contains two sample OU definitions: one for importing groups into the system and the other for users.

1. Navigate to **System LDAP > LDAP Servers**.
2. Select the LDAP server to configure.
3. In the **LDAP OU Definitions** related list, select either the **Groups** or **Users** sample OU definition.
4. Complete the LDAP OU Definition form (see table).
5. Click **Update**.

   The system automatically tests the connection to the LDAP server.
6. Under **Related Links**, click **Browse** to view the LDAP directory records that the OU definition returns.

---

**OU Definition form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify the name the integration uses when referencing this OU. The name you enter here becomes an LDAP target in the data source record.</td>
</tr>
<tr>
<td>RDN</td>
<td>Specify the relative distinguished name of the subdirectory you want to search. This RDN is combined with the start-searching directory from the LDAP server definition to identify the subdirectory containing information for this organizational unit. For example, the sample OU definition uses the RDN value of CN=Users to search the LDAP directory <code>CN=Users,DC=service-now,DC=com</code> and any directory below this point. This field must match a subdirectory in your LDAP system.</td>
</tr>
<tr>
<td>Query field</td>
<td>Specify the name of the attribute within the LDAP server to query for records. The query field must be unique in both single and multiple domain instances. For best results, use email addresses or other credentials that uniquely identify the user in a multiple domain instance. Active Directory uses the <code>sAMAccountName</code> attribute. Other LDAP servers tend to use the <code>cn</code> attribute. Note: The Query field must map to the User ID field in the User [sys_user] table. For example, if an Active Directory user logs in as <code>joe.example</code>, there must be a user record with a User ID value of <code>joe.example</code> and an LDAP record with an sAMAccountName value of <code>joe.example</code>.</td>
</tr>
</tbody>
</table>
### Example organizational unit definitions

Suppose you have an LDAP server with the following directory structure:

- dc=my-domain,dc=com
  - ou=Groups
    - cn=Development
    - cn=HR
    - cn=Sales
  - ou=Users
    - ou=Development
    - ou=HR
    - ou=Sales

Further suppose that you want to exclude the HR group and HR users from the application. Do the following:

1. Create an LDAP server record with a starting search directory of dc=my-domain,dc=com.
2. Create an OU definition record for ou=Groups with a filter to exclude cn=HR.
3. Create an OU definition record for ou=Users with a filter to exclude ou=HR.

If you do not specify additional attributes or filters with an OU definition, the LDAP query returns the entire sub-tree from the starting directory and RDN.

In these examples, an OU definition with the RDN value of ou=Groups and no filter would have returned all groups. Likewise, an OU definition with the RDN value of ou=Users and no filter would have returned all users and child organizational units.
Create a data source for LDAP
Each LDAP organizational unit (OU) definition has its own related list of data sources.

Role required: admin

**Note:** Both the LDAP Server and LDAP OU Definition must be active for the test load action to function properly. When the test load is activated for the first time, the system samples up to 20 records to determine the length of the import set fields. If the sampled records do not contain values for the User ID field, the system sets the field length for all subsequent imports to the default length of 40. The import truncates any imported data that exceeds the import set table field length. Additionally, the User ID field is truncated to a maximum of 40 characters. Be aware that the 20 loaded records cannot be transformed and are for testing purposes only. If the test records contain values for the User ID field, the field length is set based on the field length of the longest user ID in the test records.

To create a new data source:

1. Navigate to System LDAP > LDAP Servers.
2. Select the LDAP server to configure.
3. In the LDAP OU Definitions related list, select an item, such as Groups or Users.
4. In the Data Sources related list, click New.
5. Complete the Data Source form (see table).
6. Click Submit.
7. Under Related Links, click Test Load 20 Records to test whether the data source can bring LDAP data into the import table.

**Data Sources form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify the name the integration uses when referencing this data source.</td>
</tr>
<tr>
<td>Import set table name</td>
<td>Enter the name of the staging table where the system temporarily places the imported LDAP records and attributes. Review this table to view imported LDAP records. You can use the same import set table name for all LDAP data sources.</td>
</tr>
<tr>
<td>Type</td>
<td>Select LDAP to indicate the imported data is LDAP data. After you select the type LDAP, the form displays the LDAP target field.</td>
</tr>
<tr>
<td>LDAP target</td>
<td>Select the LDAP OU definition associated with this data source.</td>
</tr>
</tbody>
</table>

**Auto provision LDAP users**
You automatically provision users who are in the LDAP server but not yet in your instance.

Role required: admin

- Create the following properties in the System Properties [sys_properties] table:

**LDAP properties**

<table>
<thead>
<tr>
<th>LDAP property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.ldap.authentication</td>
<td>Enables LDAP authentication by using LDAP to authenticate users. Set this property to true (the default value).</td>
</tr>
<tr>
<td>LDAP property</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>glide.ldap.user.autopropvision</td>
<td>Enables LDAP the system to automatically create users in the User [sys_user] table when the user exists in LDAP but is not yet in the instance. Set this property to true (the default value).</td>
</tr>
</tbody>
</table>

Both of these properties must be set to true for auto-provisioning to work.

**LDAP integration via MID Server**

Administrators can integrate using an LDAP data source over a Management, Instrumentation, and Discovery (MID) Server.

The MID Server enables communication and movement of data between the Now Platform and external applications, data sources, and services. For details on installing a MID Server, see MID Server installation.

Using a MID Server to establish an LDAP connection prevents you from having to expose the LDAP server to external network traffic. It eliminates the need to establish a VPN tunnel between your LDAP server and datacenters. The MID Server user must have the user_admin role to be able to read LDAP server configuration records.

**Note:** The MID Server does not allow using the UI action `<instance>/sys_ui_action.do?sys_id=1b4f7ef30a0001060058e223c9a5744c` to refresh user and group records from LDAP.

A MID Server connection communicates over HTTP on port 80 by default. This communication channel does not require a certificate. The connection between the MID Server and the instance is over HTTPS (port 443). The instance connects to the LDAP server directly, using LDAP or LDAPS. This connection can either be over the internet or through a VPN tunnel.

**Note:** LDAP cannot communicate via the MID Server with password authentication.

For a secure communication over SSL, you must add an SSL certificate for the MID Server. Change the LDAP server URL from LDAP to LDAPS and change to port 636.

**Note:** If you create a new LDAP server, the MID Server SSL flag sets to false by default. You can ignore this behavior.

To set connection properties for a specific LDAP server, see Define an LDAP server.

Configure LDAP connection monitoring

Change or disable LDAP connection monitoring and notifications.

Role required: admin

© 2021 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
The instance automatically sends an email to users configured in the LDAP Admins group when an LDAP server connection fails. This uses the email notification, which is launched by the **LDAP Connection Test** scheduled job. This email notification is enabled by default.

**Note:** The instance does not send the email notification unless there is at least one member in the LDAP Admins group. Make sure to populate this group with the users you want to receive the email.

By default, the scheduled job tests the connection every 15 minutes. To change this interval or disable monitoring:

1. Navigate to **System Definition > Scheduled Jobs**.
2. Open **LDAP Connection Test**.
3. Do one of the following:
   - Change the interval in the **Repeat Interval** field.
   - Disable monitoring by clearing the **Active** check box.

Import binary data through a MID Server

As an administrator, you can import binary large object (BLOB) data with an LDAP integration through the MID Server.

**Role required: admin**

1. Add the name of the LDAP column you want to import binary data from to the system property `glide.ldap.binary_attributes`.
2. Add a MID Server property with the Name `glide.ldap.binary_attributes` and the same value you set for the system property.

Troubleshooting LDAP integration via MID Server

You may encounter issues in the following areas while integrating LDAP via MID Server.

You can troubleshoot these issues by viewing the outputs found in the External Communication Channel (ECC) Queue (**Discovery > Output and Artifacts > ECC Queue**).

**Test Connection Issues**

When defining OUs within the server, there is a **Test connection** related list that is used to verify the LDAP connection. When you click this link, the ECC Queue should show a single output message with a topic name of `LDAPConnectionTesterProbe`. After the test has completed on the MID Server, the ECC Queue should show an input message with the same topic name. If the **Name** column for the input message shows `true`, the test was successful. Drill down into the record to view the payload and ensure it does not contain error messages.

**Browse Issues**

When defining OUs within the server, there is a **Browse** related list that is used to view the LDAP directory records that the OU definition returns. When you click this link, the ECC Queue should show a single output message with a topic name of `LDAPBrowseProbe`. After data has been returned from the MID Server, the ECC Queue should show
an input message with the same topic name. If the **Name** column for the input message shows **true**, the test was successful. Drill down into the record to view the payload and ensure it does not contain error messages.

**Load Import Issues**

When uploading data (for example, using the Test Load 20 Records feature), the ECC Queue should show a single output message with a topic name of **LDAPProbe**.

After data has been returned from the MID Server, the ECC Queue should show another input message called **LDAPProbeCompleted**. The **Name** column for this input message shows the total number of records returned.

An additional input messages, also named **LDAPProbe**, is displayed. The **Name** column for this input message displays the highest record number in the batch. If the total number of records returned is 258 and the batch size is 200 (the default), two LDAPProbe (200, 258) incoming messages will be received, and one LDAPProbeCompleted (258) incoming message will be received.

Drill down into the record to view the payload and ensure it does not contain error messages.

![LDAPProbe and LDAPProbeCompleted messages](image)

**Import Load**

Also keep an eye out for an output message called **LDAPProbeError**.

![LDAPProbeError message](image)

**Error message**

Click the link in the **Name** column to view the details of the error.

**LDAP paging**

LDAP paging does not work if the paging size on the LDAP server is less than 1000. Set the MID Server property **glide.ldap.max_results** to a value less than or equal to the LDAP server paging size.

**LDAP fails to import binary data**

To import binary data via LDAP, such as a user photo, you must include the binary attribute in the MID Server property **glide.ldap.binary_attributes**. For the user photo example, the attribute may be **jpegphoto**.

**Import and map data**

LDAP import maps match fields in your LDAP database to fields in your instance.

---

Note: LDAP mapping has a performance effect, so the recommended approach is to schedule it during off-peak hours, or process a few records at a time to maintain system availability.
Define a transform map that only imports the needed or required attributes. Depending on the version of the instance you are using, the method for specifying LDAP mapping relationships varies.

The easiest way to know whether or not you are running a version which uses the System LDAP application for LDAP integration is to find the application from the application navigator.

The **Run Business Rules** option is applied only for the target table. Only transform maps associated to the target table run the business rules associated with different tables. If you are updating a user group and have business rules running on a user group table, the group must have roles defined.

### LDAP import mapping options

<table>
<thead>
<tr>
<th>System LDAP application?</th>
<th>Map</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Use a transform map to specify your mapping.</td>
</tr>
<tr>
<td>No</td>
<td>Use a LDAP legacy import map to specify your mapping, or the default LDAP transform that is included in baseline instances. Remember to adjust the <strong>Coalesce</strong> field to match against the correct fields.</td>
</tr>
</tbody>
</table>

### Scheduled imports

A scheduled import allows administrators to import LDAP data on a regular schedule. By default, the LDAP integration includes two sample scheduled imports:

- Example LDAP User Import
- Example LDAP Group Import

Neither example is active by default. Change these scheduled imports to meet your company's business needs.

### LDAP transform maps

The transform map moves data from the import set table to the target table (User or Group).

The LDAP integration uses standard import sets and transform maps. You can also create custom LDAP transform maps.

**Important:** Whether you select or create custom LDAP transform maps, there should be one active transform map for a set of source and target tables. Enabling multiple transform maps for the same source and target tables can produce duplicate entries in the target table unless you coalesce against the matching fields.

### Default LDAP transform maps

By default, the system provides two transform maps for LDAP data.

<table>
<thead>
<tr>
<th>Transform Map</th>
<th>Source Table</th>
<th>Target Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP User Import</td>
<td>[ldap_import]</td>
<td>[sys_user]</td>
<td>Default transform map for creating user records from LDAP credentials as part of LDAP on-demand login. Contains mappings for an Active Directory LDAP server.</td>
</tr>
</tbody>
</table>
## Transform Map

<table>
<thead>
<tr>
<th>Transform Map</th>
<th>Source Table</th>
<th>Target Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP Group Import</td>
<td>[ldap_group_import]</td>
<td>[sys_user_group]</td>
<td>Default transform map for creating group records from LDAP OUs. Contains mappings for an Active Directory LDAP server.</td>
</tr>
</tbody>
</table>

**Note:** By default, the system does not have a transform map for LDAP department records.

### Requirements for custom LDAP transform maps

If you choose to create a custom transform map, the transform map must meet the following mapping requirements.

#### Requirements for custom LDAP transform maps

<table>
<thead>
<tr>
<th>Source Table</th>
<th>Source Field</th>
<th>Target Table</th>
<th>Target Field</th>
<th>Coalesce</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ldap_import</td>
<td>u_source</td>
<td>sys_user</td>
<td>source</td>
<td>false</td>
<td>The <code>u_source</code> field identifies the LDAP DN of the imported user or group. The system uses this field to determine that a user requires LDAP authentication, to find a user's manager, and to put users into groups.</td>
</tr>
</tbody>
</table>

If LDAP integrates to Active Directory, select `u_samaccountname` as the source field. If other LDAP directories are used, select `u_dn` or `u_cn` as the source field.

### Differences between LDAP transform maps and legacy import maps

When specifying LDAP mapping relationships using transform maps, there is a major difference in how reference fields are set for manager and department.

When using a transform map, it is necessary to use a transform script to create references. This is because the value associated with an LDAP attribute like "manager" is the distinguished name (DN) of the manager.
Without some extra logic in place, the result is the creation of a user record with a manager name that is the distinguished name of that user in LDAP. The integration includes a transform script to facilitate the creation of these references. The default transform map "LDAP User Import" includes transform scripts for these references.

**Existing mapping relationships**

When updating legacy import maps to transform maps, you can retain the LDAP mapping relationships that existed prior to the addition of the System LDAP application. The LDAP server has a **Map** field that is a reference to the legacy import map.

**Note:** By default this field is hidden, so you have to configure the form to display it.

If you want to transition to using a transform map, clear the reference to the legacy import map.

**LDAP import map settings**

Verify and use attributes to limit the fields the integration imports from the LDAP source. Additionally, it is important to map the user_name field to the LDAP attribute that contains the user's login ID. For Active Directory this is usually the sAMAccountName attribute. If you would like to import and coalesce on a binary attribute (such as objectSID or objectGUID), you have to create a custom transform script.

**Note:** Any value mapped to the user_name field must be unique.

If you do not specify a transform map (such as LDAP User Import), the integration uses the following default mappings:

**LDAP import default mapping**

<table>
<thead>
<tr>
<th>User field or variable</th>
<th>LDAP attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>user_name</td>
<td>sAMAccountName</td>
</tr>
<tr>
<td>email</td>
<td>mail</td>
</tr>
<tr>
<td>home_phone</td>
<td>homePhone</td>
</tr>
<tr>
<td>mobile_phone</td>
<td>mobile</td>
</tr>
<tr>
<td>first_name</td>
<td>givenName</td>
</tr>
<tr>
<td>last_name</td>
<td>sn</td>
</tr>
<tr>
<td>title</td>
<td>title</td>
</tr>
<tr>
<td>department</td>
<td>department</td>
</tr>
<tr>
<td>manager</td>
<td>manager</td>
</tr>
<tr>
<td>middle_name</td>
<td>initials</td>
</tr>
<tr>
<td>u_memberof</td>
<td>groups</td>
</tr>
<tr>
<td>u_member</td>
<td>members</td>
</tr>
<tr>
<td>u_manager</td>
<td>manager</td>
</tr>
</tbody>
</table>
**LDAP data transformation**

If an LDAP attribute contains simple data, the transform map links an imported LDAP attribute to an appropriate field in the target table (User or Group). For example, sample data in the sAMAccountName attribute maps to the **User ID** field in the User table.

If the imported LDAP data maps to a reference field, the instance searches for an existing matching record. If no matching record exists, the instance creates a new record for the reference field unless the field mapping specifies otherwise.

For example, suppose the LDAP attribute l maps to the **Location** reference field in the User table. Whenever the import brings in an attribute value that does not match an existing location record value, the transform map creates a new location record. The new location record has the same value as the imported attribute, and the imported user record now has a link to the new location record.

However, there are times when LDAP attribute returns a distinguished name (DN), which is essentially a reference to another record within the LDAP directory. For example, the manager attribute typically contains the distinguished name for the manager of the current LDAP directory entry. An imported DN typically uses a long text string such as: `cn=Beth Anglin,ou=Users,dc=my-domain,dc=com`.

**Warning:** Make sure your target fields are long enough to contain a DN. Many text fields use the default length of 40, which may not be long enough for some DN values. The ServiceNow system truncates any value that exceeds the field length.

Administrators do not typically want the system to create new users from the DN value because the new user has no association with an existing user. Instead, administrators want the import to locate the manager's existing user record and associate it with the newly imported user. The **LDAPUtils** script include contains the **setManager** and **processManagers** functions that can parse a DN and search for an existing user. For best results, use these functions to create a custom transform map.

For example, the **LDAP User Import** transform map script calls the **setManager** function:

```java
// The manager coming in from LDAP is the DN value for the manager. // The line of code below will locate the manager that matches the // DN value and set it into the target record. If you are not // interested in getting the manager from LDAP then remove or // comment out the line below
ldapUtils.setManager (source , target ) ;
```

In some cases, the integration imports a user's record before importing the associated manager's user record. To handle such cases, you may want to call the **processManagers** function after the transform completes. For example, the **LDAP User Import** transform map uses an **onComplete** transform script to call the **processManagers** function.

```java
// It is possible that the manager for a user did not exist in the database when // the user was processed and therefore we could not locate and set the // manager field. // The processManagers call below will find all those records for which a manager could // not be found and attempt to locate the manager again. This happens at the end of the // import and therefore all users should have been created and we should be able to // locate the manager at this point
ldapUtils.processManagers ( ) ;
```

Remove or comment out the **setManager** and **processManagers** function calls if your LDAP integration does not use the manager attribute.
LDAP scripting
Create custom transform maps, scripts, and business rules to specify requirements when importing data.

Custom transform maps should include **onStart** and **onAfter** transform scripts.

The **onStart** script should call the **LDAPUtils** script include and start logging. For example, the **LDAP User Import** transform map has an **onStart** script that uses this code:

```javascript
gs.include ( "LDAPUtils" ) ;
var ldapUtils  = new LDAPUtils ( ) ;
ldapUtils. setLog (log ) ;
```

The **onAfter** script should call the **addMembers** function. For example:

```javascript
ldapUtils.addMembers (source , target ) ;
```

Set disabled Active Directory users to inactive
Use the following script to automatically deactivate users when the associated AD user is disabled.
Role required: admin
You can identify disabled Active Directory users by checking the value of the **userAccountControl** attribute. This rule executes whenever the **userAccountControl** value changes and deactivates user accounts if the **User Account Control** signifies a disabled AD account.

Use the following script to automatically deactivate users when the associated AD user is disabled.

1. Configure the User form and create a new integer field called **User Account Control**.
2. Add mapping for userAccountControl (external) to the new field.
3. Create a new business rule with the following properties:

<table>
<thead>
<tr>
<th>Business rule field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Disable AD Users</td>
</tr>
<tr>
<td>Table</td>
<td>User [sys_user]</td>
</tr>
<tr>
<td>When</td>
<td>Before</td>
</tr>
<tr>
<td>Condition</td>
<td>current.u_user_account_control.changes()</td>
</tr>
</tbody>
</table>

The Script field should contain the following:

```javascript
var disabledFlag = 2;
//perform a bitwise comparison on userAccountControl to see if the 2 bit flag is enabled
if (current.u_user_account_control && disabledFlag) {
    gs.log('Disabling user: ' + current.user_name + 'userAccountControl=' + current.u_user_account_control);
    current.active='false';
    current.locked_out='true';
}
```

Assign LDAP field values
You can use a script to assign a value to any field for which there is a field mapping.

For example, to assign a value to the sys_user.company field, create a field map for the company field and add a transform script of:

```javascript
company = "Don's Sporting Goods";
```
Exclude particular LDAP users

If you cannot completely filter the LDAP user list using LDAP filter properties, you can exclude users with a map script.

After you have run the logic to identify a user that should not be imported, set the user_name field to an empty string and this user will not be imported.

```javascript
user_name='';
```

One way to identify users to filter out is to look for a string in the distinguishedName attribute. For example, this script excludes accounts that are not in a Users OU. You might use this script if you have too many Users OU to include in the target OU LDAP Option.

```javascript
//vdn is a variable mapped to distinguishedName
gs.include("LDAPUtils");
var vdn = source.getElement(this.distinguishedName);
if (vdn.indexOf('OU=Users')<0) {
  user_name='';
  gs.log('LDAP Import Skipping User: ' + vdn);
}
```

A more complex method of filtering is to use regular expressions.

```javascript
//vcn is a variable mapped to cn
//vdn is a variable mapped to distinguishedName
//c is the regular expression string
//c=/^[a-z][a-z][a-z][0-9][0-9][0-9]$/;
gs.include("LDAPUtils");
var vdn = source.getElement(this.distinguishedName);
var vcn = source.getElement(this.cn);
var c = /^\[a-z\][a-z][0-9][0-9][0-9]$/;
var nvcn = vcn.toLowerCase();
//test to see if the cn is in the form of 3 letters followed by 3 numbers, only import these
if (c.test(nvcn)) {
  user_name = nvcn;
} else {
  gs.log("LDAP import rejected username: " + vcn + " for DN: " + vdn);
  user_name = "";
}
```

Set choice action for reference field imports

The LDAP transform map determines how fields in the Import Set table map to fields in existing tables such as Incident or User.

Role required: admin

If the LDAP transform map updates a field in the import set table, the integration automatically creates a new record whenever there is a new record in the LDAP data. If the LDAP transform map updates a reference field storing data from another table, the administrator can choose to create, ignore, or reject new LDAP records.

For example, if the integration receives a new department record that does not match any existing department, you may want to update all of the other LDAP record fields without creating a new department record in the instance. The transform map allows you to set the record creation options for each reference field.

1. Navigate to System LDAP > Transform Maps.
2. In the Field Maps related list, select one of the following actions from the **Choice action** field:

   • **create** – creates a new reference field record if a matching record does not exist.
   • **ignore** – ignores new records in the reference field and completes processing of all other fields in the transform map.
   • **reject** – stops the transform for the entire record.

   **Note:** The field map only displays the **Choice action** field for reference fields.

**Verify LDAP mapping**

After creating an LDAP transform map, refresh the LDAP data to verify the transform map works as expected.

**Role required:** admin

1. Navigate to **System LDAP > Scheduled Loads**.
2. Click your LDAP import job.
3. Click **Execute Now**.

**LDAP integration troubleshooting**

If you are integrating your LDAP server and have questions, these items may help you troubleshoot the issue.

**Preliminary checks**

- If the LDAP is unavailable, users cannot log in to the instance. A good practice is to have local accounts for administrators so that if the LDAP is down, administrators can still access the instance.
- Check the service account to ensure that it is not expired or locked out.
- Check the format of the username. Instead of using just the username, try using the domain with the username, or username@domain.
- Verify that you have changed the **system_id** entry on the **ldap_server_config** record. If you modify the **system_id** unintentionally with an update set, **system_id** points to the wrong node for the target instance and does not work.

**Error codes**

The LDAP log file lists industry standard error codes for both LDAP and Active Directory (AD). The LDAP log file is contained in the wrapper file. The LDAP error codes are two-digit numbers, while the Active Directory error codes are three-digit numbers. For a list of the most-common error codes, see [LDAP Error Codes](#).

**Multiple domain integration**

You can integrate multiple domains within the same forest or in completely non-trusted domains. It is recommended that you create a separate **LDAP server record** for each domain. Each LDAP server record must point to a domain controller for that given domain. This means you will have to allow connections to each of the domain controllers. Multiple AD forests through LDAP with one LDAP account is not supported.

When you expand to more than one domain, it is critical that you identify unique LDAP attributes for the application usernames and import coalesce values. A common unique coalesce attribute for Active Directory is **objectSid**. Unique usernames will vary based on your LDAP data design. Common unique attributes are **email** or **userPrincipalName**.
Incoming records

See LDAP transform maps to set how the integration processes incoming LDAP records that are missing matching values in reference fields.

Common authentication errors

- User Cannot Log In (Invalid DN)
- Invalid CN
- Invalid Connection

Automatic LDAP connection tests

You can manually test connections to LDAP servers or allow ServiceNow to automatically test the connections.

The system tests the connection automatically:

- Every time a user opens the LDAP Server form.
- Through the LDAP Connection Test scheduled job, which runs every 15 minutes by default.

  You can change how often this scheduled job runs. If this scheduled job is not able to establish a connection, a new one-time schedule job retries the connection test after either five minutes, or half the repeat interval value in the scheduled job, whichever occurs first.

Error messages appear on the form if there are any issues connecting to the LDAP server. Also supported are test connections for servers behind a MID server.

View the LDAP monitor

You can view current information about LDAP servers and listeners using LDAP monitor.

Role required: admin

The available states are:

- Active
- Inactive
- Error
- Active (Shutting down...)
- Error (Shutting down...)

In addition to its current state, the monitor also shows:

- The last message detected by the listener, such as waiting for LDAP changes, error connecting, and so forth.
- The last LDAP user change, such as new user, updated user, and so forth.
- The last error that occurred.
To view LDAP monitor:

Navigate to **LDAP > System LDAP > LDAP Monitor.**

See the table for descriptions of the properties and fields in the screen.

<table>
<thead>
<tr>
<th><strong>LDAP monitor</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td>Refresh</td>
</tr>
<tr>
<td>Connection Status</td>
</tr>
<tr>
<td>Field</td>
</tr>
<tr>
<td>-----------------------</td>
</tr>
<tr>
<td>LDAP Server Properties</td>
</tr>
<tr>
<td>Server URL</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Starting search directory</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>MID Server Status</td>
</tr>
<tr>
<td>LDAP Listener Status</td>
</tr>
<tr>
<td>Current Status</td>
</tr>
<tr>
<td>Last Info Message</td>
</tr>
<tr>
<td>Last Change</td>
</tr>
<tr>
<td>Last Error</td>
</tr>
</tbody>
</table>
**LDAP error codes**

The LDAP Log file lists industry standard error codes for both LDAP and Active Directory (AD).

### Standard error codes

#### Standard LDAP errors

<table>
<thead>
<tr>
<th>Error / data code</th>
<th>Text</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>LDAP_SUCCESS</td>
<td>Indicates the requested client operation completed successfully.</td>
</tr>
<tr>
<td>2</td>
<td>LDAP_PROTOCOL_ERROR</td>
<td>Indicates that the server has received an invalid or malformed request from the client.</td>
</tr>
<tr>
<td>3</td>
<td>LDAP_TIMELIMIT_EXCEEDED</td>
<td>Indicates that the operation's time limit specified by either the client or the server has been exceeded. On search operations, incomplete results are returned.</td>
</tr>
<tr>
<td>4</td>
<td>LDAP_SIZELIMIT_EXCEEDED</td>
<td>Indicates that in a search operation, the size limit specified by the client or the server has been exceeded. Incomplete results are returned.</td>
</tr>
<tr>
<td>5</td>
<td>LDAP_COMPARE_FALSE</td>
<td>Does not indicate an error condition. Indicates that the results of a compare operation are false.</td>
</tr>
<tr>
<td>6</td>
<td>LDAP_COMPARE_TRUE</td>
<td>Does not indicate an error condition. Indicates that the results of a compare operation are true.</td>
</tr>
<tr>
<td>7</td>
<td>LDAP_AUTH_METHOD_NOT_SUPPORTED</td>
<td>Indicates that during a bind operation the client requested an authentication method not supported by the LDAP server.</td>
</tr>
<tr>
<td>8</td>
<td>LDAP_STRONG_AUTH_REQUIRED</td>
<td>Indicates one of the following: In bind requests, the LDAP server accepts only strong authentication. In a client request, the client requested an operation such as delete that requires strong authentication. In an unsolicited notice of disconnection, the LDAP server discovers the security protecting the communication between the client and server has unexpectedly failed or been compromised.</td>
</tr>
<tr>
<td>9</td>
<td>Reserved</td>
<td></td>
</tr>
<tr>
<td>Error / data code</td>
<td>Text</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>10</td>
<td>LDAP_REFERRAL</td>
<td>Does not indicate an error condition. In LDAPv3, indicates that the server does not hold the target entry of the request, but that the servers in the referral field may.</td>
</tr>
<tr>
<td>11</td>
<td>LDAP_ADMINLIMIT_EXCEEDED</td>
<td>Indicates that an LDAP server limit set by an administrative authority has been exceeded.</td>
</tr>
<tr>
<td>12</td>
<td>LDAP_UNAVAILABLE_CRITICAL_EXTENSION</td>
<td>Indicates that the LDAP server was unable to satisfy a request because one or more critical extensions were not available. Either the server does not support the control or the control is not appropriate for the operation type.</td>
</tr>
<tr>
<td>13</td>
<td>LDAP_CONFIDENTIALITY_REQUIRED</td>
<td>Indicates that the session is not protected by a protocol such as Transport Layer Security (TLS), which provides session confidentiality.</td>
</tr>
<tr>
<td>14</td>
<td>LDAP_SASL_BIND_IN_PROGRESS</td>
<td>Does not indicate an error condition, but indicates that the server is ready for the next step in the process. The client must send the server the same SASL mechanism to continue the process.</td>
</tr>
<tr>
<td>15</td>
<td></td>
<td>Not used.</td>
</tr>
<tr>
<td>16</td>
<td>LDAP_NO_SUCH_ATTRIBUTE</td>
<td>Indicates that the attribute specified in the modify or compare operation does not exist in the entry.</td>
</tr>
<tr>
<td>17</td>
<td>LDAP_UNDEFINED_TYPE</td>
<td>Indicates that the attribute specified in the modify or add operation does not exist in the LDAP server's schema.</td>
</tr>
<tr>
<td>18</td>
<td>LDAP_INAPPROPRIATE_MATCHING</td>
<td>Indicates that the matching rule specified in the search filter does not match a rule defined for the attribute's syntax.</td>
</tr>
<tr>
<td>19</td>
<td>LDAP_CONSTRAINT_VIOLATION</td>
<td>Indicates that the attribute value specified in a modify, add, or modify DN operation violates constraints placed on the attribute. The constraint can be one of size or content (string only, no binary).</td>
</tr>
<tr>
<td>20</td>
<td>LDAP_TYPE_OR_VALUE_EXISTS</td>
<td>Indicates that the attribute value specified in a modify or add operation already exists as a value for that attribute.</td>
</tr>
<tr>
<td>Error / data code</td>
<td>Text</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>21</td>
<td>LDAP_INVALID_SYNTAX</td>
<td>Indicates that the attribute value specified in an add, compare, or modify operation is an unrecognized or invalid syntax for the attribute.</td>
</tr>
<tr>
<td>22-31</td>
<td>Not used.</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>LDAP_NO_SUCH_OBJECT</td>
<td>Indicates the target object cannot be found. This code is not returned on following operations: Search operations that find the search base but cannot find any entries that match the search filter. Bind operations.</td>
</tr>
<tr>
<td>33</td>
<td>LDAP_ALIAS_PROBLEM</td>
<td>Indicates that an error occurred when an alias was dereferenced.</td>
</tr>
<tr>
<td>34</td>
<td>LDAP_INVALID_DN_SYNTAX</td>
<td>Indicates that the syntax of the DN is incorrect. (If the DN syntax is correct, but the LDAP server’s structure rules do not permit the operation, the server returns code 53: LDAP_UNWILLING_TO_PERFORM.)</td>
</tr>
<tr>
<td>35</td>
<td>LDAP_IS_LEAF</td>
<td>Indicates that the specified operation cannot be performed on a leaf entry. (This code is not currently in the LDAP specifications, but is reserved for this constant.)</td>
</tr>
<tr>
<td>36</td>
<td>LDAP_ALIAS_DEREF_PROBLEM</td>
<td>Indicates that during a search operation, either the client does not have access rights to read the aliased object’s name or dereferencing is not allowed.</td>
</tr>
<tr>
<td>37-47</td>
<td>Not used.</td>
<td></td>
</tr>
<tr>
<td>48</td>
<td>LDAP_INAPPROPRIATE_AUTH</td>
<td>Indicates that during a bind operation, the client is attempting to use an authentication method that the client cannot use correctly. For example, either of the following cause this error: The client returns simple credentials when strong credentials are required...OR...The client returns a DN and a password for a simple bind when the entry does not have a password defined.</td>
</tr>
<tr>
<td>49</td>
<td>LDAP_INVALID_CREDENTIALS</td>
<td>Indicates that during a bind operation one of the following occurred: The client passed either an incorrect DN or password, or the password is incorrect because it has expired, intruder detection has locked the account, or another similar reason. See the data code for more information.</td>
</tr>
<tr>
<td>Error / data code</td>
<td>Text</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>49 / 52e</td>
<td>AD_INVALID CREDENTIALS</td>
<td>Indicates an Active Directory (AD) AcceptSecurityContext error, which is returned when the username is valid but the combination of password and user credential is invalid. This is the AD equivalent of LDAP error code 49.</td>
</tr>
<tr>
<td>49 / 525</td>
<td>USER NOT FOUND</td>
<td>Indicates an Active Directory (AD) AcceptSecurityContext data error that is returned when the username is invalid.</td>
</tr>
<tr>
<td>49 / 530</td>
<td>NOT_PERMITTED_TO_LOGON_AT_THIS_TIME</td>
<td>Indicates an Active Directory (AD) AcceptSecurityContext data error that is logon failure caused because the user is not permitted to log on at this time. Returns only when presented with a valid username and valid password credential.</td>
</tr>
<tr>
<td>49 / 531</td>
<td>RESTRICTED_TO_SPECIFIC_MACHINES</td>
<td>Indicates an Active Directory (AD) AcceptSecurityContext data error that is logon failure caused because the user is not permitted to log on from this computer. Returns only when presented with a valid username and valid password credential.</td>
</tr>
<tr>
<td>49 / 532</td>
<td>PASSWORD_EXPIRED</td>
<td>Indicates an Active Directory (AD) AcceptSecurityContext data error that is a logon failure. The specified account password has expired. Returns only when presented with valid username and password credential.</td>
</tr>
<tr>
<td>49 / 533</td>
<td>ACCOUNT_DISABLED</td>
<td>Indicates an Active Directory (AD) AcceptSecurityContext data error that is a logon failure. The account is currently disabled. Returns only when presented with valid username and password credential.</td>
</tr>
<tr>
<td>49 / 568</td>
<td>ERROR_TOO_MANY_CONTEXT_IDS</td>
<td>Indicates that during a log-on attempt, the user's security context accumulated too many security IDs. This is an issue with the specific LDAP user object/account which should be investigated by the LDAP administrator.</td>
</tr>
<tr>
<td>49 / 701</td>
<td>ACCOUNT_EXPIRED</td>
<td>Indicates an Active Directory (AD) AcceptSecurityContext data error that is a logon failure. The user's account has expired. Returns only when presented with valid username and password credential.</td>
</tr>
<tr>
<td>Error / data code</td>
<td>Text</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>49 / 773</td>
<td>USER MUST RESET PASSWORD</td>
<td>Indicates an Active Directory (AD) AcceptSecurityContext data error. The user's password must be changed before logging on the first time. Returns only when presented with valid user-name and password credential.</td>
</tr>
<tr>
<td>50</td>
<td>LDAP_INSUFFICIENT_ACCESS</td>
<td>Indicates that the caller does not have sufficient rights to perform the requested operation.</td>
</tr>
<tr>
<td>51</td>
<td>LDAP_BUSY</td>
<td>Indicates that the LDAP server is too busy to process the client request at this time but if the client waits and resubmits the request, the server may be able to process it then.</td>
</tr>
<tr>
<td>52</td>
<td>LDAP_UNAVAILABLE</td>
<td>Indicates that the LDAP server cannot process the client's bind request, usually because it is shutting down.</td>
</tr>
<tr>
<td>52e</td>
<td>AD_INVALID_CREDENTIALS</td>
<td>Indicates an Active Directory (AD) AcceptSecurityContext error, which is returned when the username is valid but the combination of password and user credential is invalid. This is the AD equivalent of LDAP error code 49: LDAP_INVALID_CREDENTIALS.</td>
</tr>
<tr>
<td>53</td>
<td>LDAP_UNWILLING_TO_PERFORM</td>
<td>Indicates that the LDAP server cannot process the request because of server-defined restrictions. This error is returned for the following reasons: The add entry request violates the server's structure rules...OR...The modify attribute request specifies attributes that users cannot modify...OR...Password restrictions prevent the action...OR...Connection restrictions prevent the action.</td>
</tr>
<tr>
<td>54</td>
<td>LDAP_LOOP_DETECT</td>
<td>Indicates that the client discovered an alias or referral loop, and is thus unable to complete this request.</td>
</tr>
<tr>
<td>55-63</td>
<td>Not used.</td>
<td></td>
</tr>
<tr>
<td>64</td>
<td>LDAP_NAMING_VIOLATION</td>
<td>Indicates that the add or modify DN operation violates the schema's structure rules. For example, The request places the entry subordinate to an alias. The request places the entry subordinate to a container that is forbidden by the containment rules. The RDN for the entry uses a forbidden attribute type.</td>
</tr>
<tr>
<td>Error / data code</td>
<td>Text</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>65</td>
<td>LDAP_OBJECT_CLASS_VIOLATION</td>
<td>Indicates that the add, modify, or modify DN operation violates the object class rules for the entry. For example, the following types of request return this error: The add or modify operation tries to add an entry without a value for a required attribute. The add or modify operation tries to add an entry with a value for an attribute which the class definition does not contain. The modify operation tries to remove a required attribute without removing the auxiliary class that defines the attribute as required.</td>
</tr>
<tr>
<td>66</td>
<td>LDAP_NOT_ALLOWED_ON_NONLEAF</td>
<td>Indicates that the requested operation is permitted only on leaf entries. For example, the following types of requests return this error: The client requests a delete operation on a parent entry. The client request a modify DN operation on a parent entry.</td>
</tr>
<tr>
<td>67</td>
<td>LDAP_NOT_ALLOWED_ON_RDN</td>
<td>Indicates that the modify operation attempted to remove an attribute value that forms the entry's relative distinguished name.</td>
</tr>
<tr>
<td>68</td>
<td>LDAP_ALREADY_EXISTS</td>
<td>Indicates that the add operation attempted to add an entry that already exists, or that the modify operation attempted to rename an entry to the name of an entry that already exists.</td>
</tr>
<tr>
<td>69</td>
<td>LDAP_NO_OBJECT_CLASS_MODS</td>
<td>Indicates that the modify operation attempted to modify the structure rules of an object class.</td>
</tr>
<tr>
<td>70</td>
<td>LDAP_RESULTS_TOO_LARGE</td>
<td>Reserved for CLDAP.</td>
</tr>
<tr>
<td>71</td>
<td>LDAP_AFFECTS_MULTIPLE_DSAS</td>
<td>Indicates that the modify DN operation moves the entry from one LDAP server to another and requires more than one LDAP server.</td>
</tr>
<tr>
<td>72-79</td>
<td>Not used.</td>
<td></td>
</tr>
<tr>
<td>80</td>
<td>LDAPOTHER</td>
<td>Indicates an unknown error condition. This is the default value for NDS error codes which do not map to other LDAP error codes.</td>
</tr>
<tr>
<td>775</td>
<td>USERACCOUNT_LOCKED</td>
<td>Indicates users are unable to log in because the user account is locked.</td>
</tr>
</tbody>
</table>
Customized error codes

Customized LDAP error codes

<table>
<thead>
<tr>
<th>Error / data code</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>10000</td>
<td>LDAP_ERROR_GENERAL</td>
</tr>
<tr>
<td>10001</td>
<td>LDAP_ERROR_MAL_FORMED_URL</td>
</tr>
<tr>
<td>10002</td>
<td>LDAP_ERROR_UNAUTHENTICATED_BIND</td>
</tr>
<tr>
<td>10300</td>
<td>LDAP_ERROR_COMMUNICATION_EXCEPTION</td>
</tr>
<tr>
<td>10301</td>
<td>LDAP_ERROR_SOCKET_TIMEOUT</td>
</tr>
<tr>
<td>10302</td>
<td>LDAP_ERROR_CONNECTION_REFUSED</td>
</tr>
<tr>
<td>10303</td>
<td>LDAP_ERROR_CONNECTION_RESET</td>
</tr>
<tr>
<td>10304</td>
<td>LDAP_ERROR_NO_ROUTE</td>
</tr>
<tr>
<td>10305</td>
<td>LDAP_ERROR_UNKNOWN_HOST</td>
</tr>
<tr>
<td>10400</td>
<td>LDAP_ERROR_SSL_EXCEPTION</td>
</tr>
<tr>
<td>10401</td>
<td>LDAP_ERROR_SSL_EMPTY_CERT_STORE</td>
</tr>
<tr>
<td>10402</td>
<td>LDAP_ERROR_SSL_CERT_NOT_FOUND</td>
</tr>
<tr>
<td>10403</td>
<td>LDAP_ERROR_SSL_CERT_EXPIRED</td>
</tr>
<tr>
<td>10500</td>
<td>LDAP_ERROR_INVALID_SEARCH_FILTER_EXCEPTION</td>
</tr>
</tbody>
</table>

Send a one-time password when the LDAP server is down

An LDAP property is available to send a one-time password to a user if the user is unable to log in because the LDAP server is down. You can also configure another property to control how long the password is valid.

Role required: admin

To receive a one-time password, the user must have notifications enabled on their user profile. The notification is an email message only. SMS messages are not supported.

Both properties are enabled by default. The default value for property that controls password validity is 10 minutes.

1. Open the list of system properties by entering `sys_properties.list` in the filter of the application navigator.
2. Find the `glide.ldap.onetime.password.enabled` property.
3. Set the property to `true`.
4. To change the password validity time for a user, set the following property to an integer number of minutes: `glide.authenticate.onetime.password.validity`.

LDAP record synchronization

Administrators can synchronize inactive, disabled, or deleted LDAP records with their LDAP records.

LDAP record synchronization is the process of detecting inactive records on the LDAP server and updating the corresponding LDAP records. Detecting inactive LDAP records involves defining consistent data indicators for each user object, importing LDAP data, and evaluating the data indicators.

A data indicator can be:
- a date field
• membership in a specific OU (identify by parsing the dn attribute), using the useraccountcontrol attribute
• a combination of these indicators

Imported data comes into the instance through import set tables where the data can be evaluated and processed.

The import process can use:

• **LDAP extraction**: a single import job to gather all user records into the import set temporary tables for evaluation
• **LDAP refresh filters**: multiple import jobs to divide different types of user records, segregating records for separate processing

**LDAP refresh filters**

Filters on the LDAP refresh process can be used to specify processing that ignores inserts of disabled users.

You can loosen the LDAP OU filter to bring all of the data in to your import set table (including inactive users) and then specify processing that ignores inserts of disabled users. The sample ‘Users’ OU definition that the instance provides in its out-of-box LDAP sample contains a filter.

This filter is important because it defines which user records are brought into the import set table to be evaluated. While achieving a smaller data load, a limitation of this filter is that it filters out inactive users, so the inactive user records are not imported into the import set temporary tables. Since there is not visibility of the inactive user records, there is no ability to evaluate the record indicators.

**LDAP OU filter**

To use filtering within the main LDAP refresh process, change the filter to bring in all of the user records. The result is that all the records will be loaded into the import set temporary table where they can be evaluated and transformed.

**Note**: There is a precaution here: because the filtering brings in all the records, you may end up with a vast amount of older inactive LDAP accounts that should not be inserted into the instance. A user record should never be created for a disabled user.

**Alternative method**

**LDAP extraction** uses a single import job to gather all user records into the import set temporary tables for evaluation.
**LDAP extraction**

An LDAP extraction process can be implemented to detect disabled users.

An extract from your LDAP source can filtered for disabled users using an active flag that can be set for every record in the import to ‘false’. Specify (‘target.active=false’) and copy into the **Script** field directly on the Table Transform Map record.

**Benefits**

Benefits to this method include:
- Simple scripting
- Existing user records are not involved in processing
- Inactive users are not loaded into a temporary import table
- No performance impact

**Drawbacks**

Drawbacks to this method include:
- An additional process is created
- The extract set must be placed in a location where your data source can access it

**Alternative method**

**LDAP refresh filters** use multiple import jobs to divide different types of user records, segregating records for separate processing.

**Inactive LDAP user accounts**

Detect that an existing, current, user account is inactive or has been disabled or deleted from an Active Directory (AD) LDAP.

A common LDAP integration issue is how to detect disabled or deleted users in an Active Directory (AD) and then deactivate them in the instance. In an Active Directory LDAP, a filter is usually set to exclude inactive users when refreshing, so the instance is not aware of users that are disabled or deleted in AD. The issue is how to detect that an existing, current user is inactive or has been deleted from AD.

| Note: | The recommended approach is to deactivate user records and all other types of records, not delete them. Each record is linked to other records, and deleting a record destroys all the relationships to those other records. Deactivating records keeps those relationships in place. |

Find inactive LDAP accounts using the userAccountControl field

Identify when an Active Directory (AD) user is deleted (or made inactive).

Role required: admin

One method is to track the active status of AD users and create a business rule to update corresponding accounts when an AD account is inactive.

1. Create a new string field on the User [sys_user] table to track the value of the AD **userAccountControl** field. For example: `u_ad_user_account`.
2. Create an LDAP transform script to set the field value.

```plaintext
target.u_ad_user_account = source.userAccountControl
```
3. Update the LDAP filter to show disabled AD accounts. Here is an example of a filter.

```
(&(objectClass=person) (sn=*)(!(objectClass=computer))(!
(userAccountControl:1.2.840.113556.1.4.803:=2)))
```

Here is an example of a replacement filter you can use.

```
(&(objectClass=person) (sn=*)(!(objectClass=computer)))
```

4. Create an onChange business rule to set the active field to false whenever the u_ad_user_account field has the value 514. '514' indicates an inactive account.

**LDAP script examples**
The following script examples assume you use an Active Directory (AD) for your LDAP server.

**userAccountControl attribute values script**
This example tests the source for the userAccountControl attribute values associated with a disabled user (514 or 546).

```javascript
//Deactivate LDAP-disabled users during transform based on 'userAccountControl' attribute
if(source.u_useraccountcontrol == '514' || source.u_useraccountcontrol == '546'){
    target.active=false;
    target.locked_out=true;
}
```

Here is an example using a bitwise check:

```javascript
if(source.u_useraccountcontrol & 2){
    active = false;
}
```

**userAccountControl attribute script**
This example examines the userAccountControl attribute but does not test for specific values. It also contains the option of reactivating LDAP user accounts.

```javascript
/*
 * Deactivate LDAP-disabled users during transform based on 'userAccountControl' attribute
 * Convert the userAccountControl attribute back to a hex value
 */
var ctrl = parseInt(source.u_useraccountcontrol, 10);
ctrl = ctrl.toString(16);

/*
 * The only digit we care about is the final one
 * A final hex digit value of '2' in 'ctrl' means disabled
 */
if(ctrl.substr(-1) == "2"){
    //Deactivate and lock the user account
    target.active = false;
}
```
onBefore transform map script

Here is an example of an onBefore transform map script. The script identifies disabled records and records being inserted. If an insert of a disabled user is occurring, then the operation transform ignores the record.

```javascript
//Ignore any insert of a disabled record as defined by the 'userAccountControl' attribute
var uc = source.u_useraccountcontrol;
if((uc == '514' || uc == '546') && action == 'insert')
  ignore = true;
}

/* Optional: Uncomment else block to reactivate and unlock the user account
else {
  target.active = true;
  target.locked_out = ctrl.substr(-2, 1) == "1";
}
*/
```

DN member script

This script example introduces flexibility by not relying on the 546 and 514 userAccountControl values, but instead checking whether the user is a member of a particular Distinguished Name (DN). You can use this script either in the Script field of the ‘Table Transform Map’ record or in an onBefore transform map script.

```javascript
//Deactivate LDAP-disabled users during transform based on OU membership in 'dn'
if(source.u_dn.indexOf('OU=Disabled Accounts') > -1)
  target.active = false;
  target.locked_out = true;
}
```

Active Directory Application Mode (ADAM)

Active Directory Application Mode (ADAM) is an Lightweight Directory Access Protocol (LDAP)-compliant directory service.

**Note:** A basic level of understanding with Microsoft Windows Server and Active Directory is needed for understanding this topic. You must also have administrator permissions on the server you are configuring for ADAM.

These are sample procedures. Due to installation and environment variations, we cannot offer direct support. We recommend working with a Microsoft consultant.

ADAM has a simple install and runs as a service on Windows operating systems. It can be fully customized and distributed as an application component or used as a stand-alone LDAP directory. ADAM uses the same technologies found on Active Directory Domain Controllers (including replication and delegation features) and has its own administration and customization features. It can be run as a Windows service. ADAM can be installed on Windows XP, 2000, 2003, and 2008 operating systems. ADAM is included as part of Windows Server 2003 R2 and Windows

**Security**

Some company security policies prohibit external vendors and partners from connecting directly to an Active Directory (AD) Domain Controller. If exposing certain AD objects or attributes to an external vendor or partner is prohibited, access to objects and attributes can be blocked using AD Security Access Control Entries (ACE or ACL). Depending on security requirements, this method can introduce complexity in the integration. Consolidating multiple domains and forests is recommended. If all LDAP imports and authentications need to be channeled through a single source, ADAM can be used as a consolidated source. With the release of Windows 2008 this functionality has been renamed to Light-Weight-Directory Service, LDS. Installation and configuration is similar to Windows Server 2003 R2.

**Recommended Knowledge**

For this task, you must understand AD, object classes and attributes. To have a successful integration, you need to be knowledgeable of the current AD object structure, familiar with Active Directory delegations, and have a strategy on how to use ADAM and for what purposes. If you are not familiar with AD or ADAM, work with your AD administrator to configure a new ADAM environment.

**Trusts**

If `userProxy` objects is used, the computer hosting ADAM needs to be a member of the domain that has the AD accounts, or a member of a trusted domain.

**Internal Connectivity**

If `userProxy` objects is used, the ADAM computer must be able to connect to the related Domain Controllers to perform proxy authentication.

*Configuring an instance with ADAM*

The first install copies the ADAM files to your computer, registers requires components, and creates the application shortcuts.

Role required: admin

By default, all of the application files are installed to `%systemroot%\ADAM`.

- Windows Server 2003 R2 - ADAM can be installed using the Control Panel > Add and Remove Programs > Optional Component Manager.

Create the first instance service which functions as the first directory service hosted by ADAM. Do one of the following:

- Run `adaministall.exe` from the ADAM folder.
• Use the **Create an ADAM instance** shortcut from the **Start Menu > Programs > ADAM** folder.
  
a) Select the **A unique instance** install option.

  **Note:** You can use this option to install an instance replica on a second server to provide a fault tolerant system.

b) Complete the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance Name</td>
<td>used primarily to identify the Windows Service name and display name</td>
</tr>
<tr>
<td>Ports</td>
<td>sets the port numbers to be used for LDAP and LDAPS Listeners. The default LDAP port is 389, LDAPS is 636. If these ports are in use on the server, the setup wizard selects new ports. Work with your network administrator to determine the best ports to use</td>
</tr>
<tr>
<td>Application Directory Partition</td>
<td>creates an application directory partition. Not needed at this step, we recommend creating the new partition now. A good practice is to use the same distinguished name as your forest or domain, but replace the highest level domain with adam instead of com or local. For example, if your forest partition is <strong>dc=myCompany,dc=com</strong>, you could create the ADAM partition as <strong>dc=myCompany,dc=adam</strong>.</td>
</tr>
<tr>
<td>File Locations</td>
<td>selects the location(s) for the ADAM partition data.</td>
</tr>
<tr>
<td>Service Account Selection</td>
<td>selects a service account that the instance runs as. For stand-alone services, you can use the default network service account. If you plan on using replicas, you need to use an account that has access to all ADAM instances.</td>
</tr>
<tr>
<td>ADAM Administrators</td>
<td>the delegation on the ADAM directory that leverages Windows integrated authentication. This is how the initial access is granted for administration. Once the initial account is granted rights, this user or group delegates rights to other Windows users or ADAM users. You can select the default to only grant admin access to the current user, or grant access to a different user or group based on your needs.</td>
</tr>
<tr>
<td>Import LDIF Files</td>
<td>the files to import. MS-UserProxy is the most important file to import, but it’s worth adding all available files since there is little overhead to the schema and you won’t have to worry about extending it later if your needs expand. Confirm the details and the wizard complete the configuration.</td>
</tr>
</tbody>
</table>
Setting up the ADAM console

Even though there are many similarities between ADAM and Active Directory, the administration can be very different since there is no **Users and Computers** management console.

Role required: **admin**

Most of the general administration is performed using the ADAM ADSI MMC console available from the **ADAM** start menu. The first time you run the ADAM ADSI console, you must connect to the partition you created.

1. Right-click the **ADAM ADSI Edit** item in the left frame.
2. Give the new connection a name and update the server name, port fields with the information used when you created the instance.
3. Select **distinguished name** or **naming context** and specify the distinguished name of the application partition you created earlier. You can connect to the **Configuration** and **Schema** partitions for advanced configuration options.
   
   You should now be able to see into the partition and the default containers for LostAndFound, NTDS Quotas, and Roles. The Roles container has not been configured yet.

Create containers and organizational units for ADAM

Objects stored in ADAM can be logically grouped into containers and organizational units (OU) just as they would in Active Directory.

Role required: **admin**

1. Right-click the root partition and select **New > Object > organizationalUnit**. You can also view the list of other objects that are available. This list varies based on the schema extensions installed when you imported the LDF files.

   **Note:** You can also view the list of other objects that are available. This list varies based on the schema extensions installed when you imported the LDF files.

2. When prompted for a value, enter the name of OU, for example **Users**.
3. The next screen displays a **More Attributes** button; use this to assign values to additional attributes. For OUs and containers, no additional values are needed.

   After creating OUs, the new OUs are listed as a child of the root object.

Delegation with ADAM

Once the OU structure is created, define the permission delegations to properly secure the objects to limited users.

As with Active Directory, there are two general ways to grant permissions:

- Add users to a group that already has the appropriate permissions assigned.
- Define new permissions on the ADAM objects.

For this task, we discuss object level permissions. Refer to the Group Administration section for information on group memberships.

Since we don’t have a Users and Computers console for ADAM, all object level permissions are defined using the Active Directory utility **DSACLs.exe**. This file is found in the ADAM program directory. When running ADAM utilities it is best to launch the ADAM Tools Command Prompt. This ensures the proper versions of the tools. DSACLCS is used to view and set object access rights.

Example: "**dsaclcs \\localhost:50010\dc=myCompany,dc=adam**" displays the permissions assigned to the root of partition **dc=myCompany,dc=adam** running on the localhost, port 50010. DSACLCS is a complex tool used to create complex delegation. Run "**DSACLCS /?**" for usage notes.
Populating ADAM Objects
ADAM Objects include User Objects, UserProxy Object, and Group Objects.

User Objects

Users can be created using the ADAM ADSI Edit console just as we did for OU creation. Users can also be administered using AD command line tools, which is beyond the scope of this document. The only mandatory attribute for new user objects is the `cn`, which is a short name or the user’s full name. There are also a wide range of optional attributes similar to Active Directory user attributes. You can access the full list of attributes by selecting properties from the user object.

UserProxy Objects

For ServiceNow LDAP integration we recommend you use UserProxy objects in ADAM which creates a proxy account that links to the related AD user account. This allows you to have ADAM authenticate logon credentials using AD usernames and passwords from the domain without ServiceNow directly connecting to the Domain Controller. UserProxy objects are very similar to AD and ADAM User objects except that do not store passwords and has an `objectSID` attribute that contains the SID from the linked AD User object. This is how the proxy works. UserProxy objects are created using the ADSIEdit console or command line tools, but this can be tedious. It is recommended that you use an automated process as defined below.

Group Objects

Groups are created using the ADSIEdit console and AD command-line tools. Group concepts are similar to AD and are used to integrate groups and members to ServiceNow. The biggest difference is ADAM groups can contain members from ADAM or from trusted AD Domains.

Automating ADAM Object Creation

If you are interested in synchronizing Active Directory accounts to ADAM, we recommend you use Microsoft ADAMSync tool. This is the most common use of ADAM for ServiceNow LDAP integration.

About Permission Delegation

ADAM contains some built-in groups with default permissions. These groups are found in the container `cn=roles,dc=myCompany,dc=adam`. These are similar to domain level groups and have rights to objects in the current partition. Similar to AD Forests you can also set a higher level of permissions using the default groups in `cn=roles,cn=configuration,dc=myCompany,dc=adam`. You must connect to the configuration partition in ADSIEdit. The Administrators group by default includes the account specified during the setup. This member is not always visible since it’s inherited through the configuration groups. Administrators have full control of all partition objects. The Readers group does not contain any members by default and has read access to all objects in the partition. The Users group is a dynamic group just as it is in Active Directory. Transitivity it includes all ADAM users created in the partition.

Testing and troubleshooting ADAM setup

The primary tool used for testing is LDP. This allows you to fully test user authentication.

Most of the object management can be completed using the ADAM ADSI Edit console which will provide access to the entire collection of objects and attributes. The highest level of control and troubleshooting ADAM services is using the Windows service created during the instance setup. The service name will vary and depends on the name of the instance created. This service must be running in order for the ADAM service to run. If you are experiencing connection problems, you should review the network configurations to ensure you have the appropriate network.
access to connect to the server and ADAM port. For each ADAM instance installed, a Windows Event Log is created. This is also a great tool for troubleshooting ADAM services.

The Windows Security Event Log is also helpful when troubleshooting userProxy authentications. All userProxy logon attempts are logged in the Security Log and reference the remote client device address, the distinguished name of the user trying to log on, and the result or status code.

**Backup and recovery with ADAM**

All ADAM data can be backed up using standard file system backup methods.

**Redundancy**

ADAM has built-in replication utilities based on the same technology as AD. A full read and write replica of an ADAM partition can exist on the same or different computer. You can use this replica in a variety of ways to provide a fault-tolerant LDAP integration with the instance. One option is to expose both partitions to the instance through the firewall and define both servers in the LDAP Properties server field.

**Use LDAPS with ADAM**

The default configuration for userProxy object authentication is to enforce LDAPS (secure LDAP) communications. LDAPS requires SSL certificates to secure the network traffic.

To remove this requirement make the following change using the ADSIEdit console connected to the configuration partition.

```plaintext
Object: CN=Directory Service, CN=Windows NT, CN=Services, CN=Configuration
Attribute: msDS-Other-Settings
Value: change RequiresSecureProxyBind from 1 (enforced) to 0 (disabled)
```

Restart the ADAM service to use the new setting.

To support secure binds and encrypt the user and password information being transmitted, a SSL certificate must be installed on the server and any LDAP client. Since there is limited and controlled uses to the ADAM service, it is feasible to use a self-signed certificate which would meet the needs without incurring certificate costs or building a Certificate Authority (CA) infrastructure. If you already have a CA, you can issue a certificate. Otherwise, create a self-signed certificate.

**Creating a Self-Signed Certificate**

To use the selfssl utility, Internet Information Services (IIS) must be installed. This service can be removed after you generate the certificate. You can get the selfssl.exe utility from the IIS Resource Kit. If IIS is already installed, create a new website so that the current sites will not be impacted during the certificate generation. Selfssl needs to temporarily attach the new self-issued certificate to a valid web site.

Selfssl is a command-line tool and has the following common parameters.

**Selfssl Parameter Descriptions**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/T</td>
<td>Adds the cert to ‘Trusted Certificates’ on the local machine</td>
</tr>
<tr>
<td>/N:cn</td>
<td>Set the common name of the certificate. This must match the fully qualified domain name of the server running the web service using the certificate</td>
</tr>
<tr>
<td>/K</td>
<td>Sets the strength of the key size in bits</td>
</tr>
<tr>
<td>/V</td>
<td>Number of days the cert is valid</td>
</tr>
</tbody>
</table>
The common name attribute should match the external name or address that the instance will use to connect to your ADAM computer. You will need to get the IIS Website site id unless you are using the default website which is 1 and does not need to be defined in the selfssl command. A sample command to generate a certificate for myCompany would be:

```
selfssl /N:CN=myCompany.externaldomain.com /K:1024 /V:3650 /S:12345 /P:50001 /T
```

This statement creates a certificate that is valid for 10 years. Set the value to any duration, but be aware the new certificate must be generated and submitted to the instance before the old one expires. We recommend making a note of the expiration date on the certificate.

Once the certificate is generated you can remove it from the website, or delete the entire web site if you created a temporary site.

### Assigning the Certificate to ADAM

To support secure binds and encrypt the user and password information being transmitted, a SSL certificate must be installed on the server and any LDAP client.

Role required: admin

Since there is limited and controlled uses to the ADAM service, it is feasible to use a self-signed certificate which would meet the needs without incurring certificate costs or building a Certificate Authority (CA) infrastructure.

To assign the certificate to ADAM.

1. Open the Certificates MMC console. Create two console connections, one for Local Computer Certificates, and the other for Local Computer Services Certificates on the new ADAM service. The new certificate can be found under Certificates (Local Computer)\Personal\Certificates.
2. Copy the certificate to the container for the ADAM service, Certificates – Service (ADAM Service Name)\ADAM_ADAM Service Name\Trusted Root Certificates \Certificates. Also copy the certificate to Certificates – Service (ADAM Service Name)\ADAM_ADAM Service Name\Personal\Certificates.
3. Open the details tab on the certificate you copied. Note the Valid from date stamp. Now assign read access to the certificate key file. Go to C:\Documents and Settings\All Users\Application Data \Microsoft\Crypto\RSA\MachineKeys and identify the certificate with the matching time stamp. Assign Read & Execute rights to the service account running ADAM. By default this is Network Service.
4. Restart the ADAM service to activate the new certificate.

### Exporting the Public Key Certificate

LDAPS clients, including the instance need the public key certificate in order to make a secure connection to ADAM.

Role required: admin

From the server certificate consoles you used above, export a public key to be used by the clients.

1. Select the certificate, right-click, select all tasks/export. Do not export the private key. Select the default DER encoded binary X.509 format and specify the export file name.
2. Install the public certificate on the LDAP clients that connect to the server using LDAPS. When prompted, add the certificate to the Trusted Root Certificate Authorities store.
Active Directory Application Mode (ADAM) Access Account

The system requires a user account to read the Active Directory Application Mode (ADAM) object information that is imported into the application instance.

Create the account by using one of the following methods:

- Create a local ADAM user account and assign it a password and assign permissions.
- Assign permission to a Windows domain account on the ADAM partition.
- Use a userProxy account.

When using ADAM as an LDAP source, you must specify the fully qualified distinguished name (FQDN) of the ADAM account in the instance's LDAP server's Login distinguished name field.

Testing LDAPS Connections

There are two console connections, one for Local Computer Certificates, and the other for Local Computer Services Certificates on the new ADAM service.

Role required: admin

1. Run LDP.exe from the ADAM install folder c:\windows\adam. Verify that the ADAM version is selected because this is not the standard Windows LDP client.
2. Open a new connection using the Connection/Connect menu. The server name must match the CN assigned to the certificate.
3. Enter the LDAPS port and select the SSL checkbox.
   The results of a successful connection are some general server information and no errors.
4. Bind (log in) to the service. To replicate typical LDAP client connections select the Simple bind option. Enter a valid ADAM user or userProxy distinguished name in the user field and the associated password.
   If you see a return message stating ‘Authenticated as:….’ then you have successfully connected using LDAPS.

Use ADAMSync to populate ADAM

Administrators use MS ADAMSync to populate LDAP directories that use MS ADAM.

Note:

This document assumes you have at least a basic level of understanding with Microsoft Windows Server, Active Directory, and ADAM and that you already have a functional Active Directory Application Mode (ADAM) instance with a partition.

These are sample procedures. Due to the complexity and the fact that it is running in your environment, we cannot offer direct support. We recommend you work with Microsoft or a Microsoft consultant if you run into any trouble.

Once ADAM has been installed and the first partition has been created, you can populate it with objects.

The following options are available:

- Manual object creation using GUI or scripts. This option is inefficient and slow.
- Integrate with Active Directory using Microsoft Integration Information Server. This option ultimately provides the most flexibility and functionality but does require some advanced configurations. There is a free version of MIIS available that is compatible with Active Directory, ADAM, and Microsoft Global Address Lists from Exchange. Unless you already have experience with MIIS we advise that you don’t attempt to implement a new environment for LDAP integration only.
- Use ADAMSync, a synchronization tool that Microsoft provides with ADAM. This is the option that is explained here.

Define ADAM user accounts
Define the following user accounts in ADAM. One is used for the instance to connect with and the other for ADAMSync.

Role required: admin

These accounts can be local ADAM User objects, UserProxy objects, or a Windows account from a trusted domain.

User Account

This account requires read-only access to the directory structure you are importing to your instance. The best way to accomplish this is to add the account to the member attribute on the Readers group found in cn=roles,dc=myCompany,dc=adam.

New ADAM User accounts are disabled by default. You will need to enable the new accounts and set a password.

1. Enable users by changing the attribute msDS-UserAccountDisabled to FALSE.
2. Right-click the user object and reset the password.
3. Test the new accounts using LDP as defined in Active Directory Application Mode (ADAM) to make sure they can connect. Use the LDAP > View/Tree option, leaving the Base DN blank to make sure you can view the objects in the directory using the new accounts. The Configuration, Schema, and the domain partition should be visible in the left pane. Traverse the domain partition. If you are using a new local ADAM account, it will show ‘No Children’ which means you don’t have read access to the objects. Verify the Setup group memberships and re-test.

ADAMSync User Account

ADAMSync uses this account to manage objects in the ADAM partition. This account requires admin level rights since it will create, update, and delete ADAM objects.

ADAMSync AD Account

ADAMSync uses this account to read the AD objects that will be synchronized to ADAM.

Set up ADAMSync

ADAMSync is included with Windows Server 2003 R2. Download and install ADAMSync if you are using a different OS.

Extending the schema

The ADAM schema needs to be extended to support ADAMSyncc.

1. Run the following command from c:\windows\adam to import the ADAMSync schema extensions. You may have to change the server:port and add credentials if the current user doesn’t have access. See the AdamSyncMetadata.ldf file for details.

   `ldifde -i -f MS-AdamSyncMetadata.LDF -s localhost:50000 -j . -c "cn=Configuration,dc=X" #configurationNamingContext`

2. Do the same with MS-AdamSchemaW2K3.ldf to support Windows 2003 attributes.

   `ldifde -i -u -f MS-AdamSchemaW2K3.LDF -s localhost:50000 -j . -c "cn=Configuration,dc=X" #configurationNamingContext`

Recommended schema changes

Here are some additional schema changes we recommend.

1. Open a new MMC console and add the ADAM Schema Snap-in.
2. Connect to the ADAM instance.

3. Expand the Classes folder and locate the userProxy class, open Properties.

4. Verify the following optional attributes on the Attributes tab, add any that do not already exist.
   - company
   - department
   - givenName
   - mail
   - physicalDeliveryOfficeName
   - sAMAccountName
   - sn
   - telephoneNumber
   - title
   - userAccountControl
   - userPrincipalName

5. Restart the ADAM Service to enable the new settings.

Install the ADAM configuration file
You can install the ADAM configuration file through the Windows command line.

Role required: admin

1. Install the configuration file.

   C:\WINDOWS\adam>adamsync /install localhost:50000 MS-AdamSyncConf-SNC.XML

2. Run the synchronization file. This will log to the console and may run for a long time.

   C:\WINDOWS\adam>adamsync /sync localhost:50000 "ou=users,dc=service-now,dc=adam" /log -

3. Review the results by using the ADSIEdit console. You should see the new objects and attributes that were created by ADAMSync.

4. Run ldap to test the UserProxy authentication.

   Automating the sync process
   Setup the sync process as a Windows Scheduled Task. You must either provide the credentials in the config file, command line, or run the Scheduled Task with an account that has access.

   Special notes
   - You can create multiple configuration files and scheduled jobs to sync ADAM from multiple sources.

     This example imports the sAMAccountName attribute which can be used as the application logon. If you are going to sync source you need to make sure you have a unique attribute value that can be used for the logon credentials. sAMAccountName is guaranteed to be unique within a domain, but not across multiple domains.
   - If you are using Microsoft Exchange, we recommend excluding cn=SystemMailbox* objects as part of the object-filter configuration.

Example ADAM configuration files
All of the configurations for ADAMSync are stored in xml files.

**Default configuration file with comments**

There is a default configuration file called MS-AdamSyncConf.xml included with the ADAMSync install. Make a copy of this file so you have a base example to refer to in the future. This example is the default configuration file with comments added.

```xml
<?xml version="1.0"?>
<doc>
  <configuration>
    <!-- Sync File Description -->
    <description>MyCompany ADAMSync Configuration</description>
    <security-mode>object</security-mode>;
    <!-- source-ad-name = fqdn of the domain controller -->;
    <source-ad-name>;fully.qualified.domain.name.of.domain.controller</source-ad-name>;
    <!-- source-ad-partition = root AD domain partition -->;
    <source-ad-partition>;dc=myCompany,dc=com</source-ad-partition>;
    <!-- source-ad-account = use this to specify an account to connect to AD -->;
    <source-ad-account>;</source-ad-account>;
    <!-- target-dn = target ADAM OU -->;
    <target-dn>;ou=servicenow users,dc=myCompany,dc=adam</target-dn>;
    <query>;
      <!-- base-dn = should be the root AD partition if you want all users -->;
      <base-dn>;dc=myCompany,dc=com</base-dn>;
      <!-- object-filter = standard ldap query format, this will grab all users -->;
      <object-filter>;(objectCategory=person)</object-filter>;
      <attributes>;
        <!-- include=userproxy requires objectSID to link back to the AD account -->;
        <include>;objectSID</include>;
        <include>;givenName</include>;
        <include>;sn</include>;
        <include>;description</include>;
        <include>;title</include>;
        <include>;company</include>;
        <include>;department</include>;
        <include>;mail</include>;
        <include>;physicalDeliveryOfficeName</include>;
        <include>;telephoneNumber</include>;
        <include>;sAMAccountName</include>;
      </attributes>;
      </query>;
      <!-- map for user-to-userproxy object types -->;
      <user-proxy>;
        <source-object-class>;user</source-object-class>;
        <target-object-class>;userProxy</target-object-class>;
      </user-proxy>;
      <schedule>;
        <aging>;
          <frequency>;0</frequency>;
          <num-objects>;0</num-objects>;
        </aging>;
        <schtasks-cmd>;</schtasks-cmd>;
      </schedule>;
  </configuration>
</doc>
```
LDAP filters configuration file

You can provide any level of filtering in the object-filter value in the configuration file. Use standard LDAP query syntax with the following XML escape characters in place of the standard operators.

- **AND** = "&" replace with &amp;#38;
- **OR** = "|" (vertical line) replace with &amp;#124;
- **NOT** = "!" replace with &amp;#33;

Reference configuration file

Here's an actual configuration file that can be referenced as a sample.

```xml
<?xml version="1.0"?>;
<doc>
<configuration>
<description>;SNCTest ADAMSync Configuration</description>
<security-mode>;object</security-mode>
<source-ad-name>;domaincontroller.service-now.com</source-ad-name>
<source-ad-partition>;dc=service-now,dc=com</source-ad-partition>
<source-ad-account>;</source-ad-account>
<account-domain>;</account-domain>
<target-dn>;ou=servicenow users,dc=service-now,dc=adam</target-dn>
<query>
<base-dn>;dc=service-now,dc=com</base-dn>
<object-filter>;(objectCategory=person)</object-filter>
<attributes>
<include>;objectSID</include>
<include>;givenName</include>
<include>;sn</include>
<include>;description</include>
<include>;title</include>
<include>;company</include>
<include>;department</include>
<include>;mail</include>
<include>;physicalDeliveryOfficeName</include>
<include>;telephoneNumber</include>
<include>;userAccountControl</include>
</attributes>
</query>
</configuration>
</doc>
```
Configure Microsoft Active Directory for secure LDAPS communication

Use certificate pairs to enable Microsoft Active Directory (AD) LDAPS communications.

**Note:** These procedures were designed and tested using Windows 2003 R2 Standard Edition and work with all versions of Windows 2003.

Secure LDAP (LDAPS) communication is similar to SSL (HTTPS) communication in that both encrypt the data between servers and clients. To accomplish this, the server and clients share common information by using certificate pairs. The server holds the private key certificate and the clients hold the public key certificate. These certificates are required to enable Microsoft Active Directory (AD) LDAPS communications.

To configure LDAPS for Active Directory you must:

- Ensure that the Active Directory domain is set up and that the instance is able to connect to the Active Directory server through the firewall.
- Verify that there is a Certificate Authority (CA) that can issue a certificate for the domain controller (DC). If you don't already have a CA infrastructure there are two options.
  - Setup a stand-alone CA to issue the certificate
  - Request a third party certificate
- If you already have a CA in place, you can generate a certificate from an internal CA.

All certificates have a defined expiration date which can be viewed in the certificate properties. If the certificate expires, all LDAPS traffic fails, and your users can no longer log into the instance. To resolve this, a new certificate must be issued and installed on your instance.

The default expiration for Microsoft CA certificates is one year. External CA certificates are usually purchased in one year increments. Note when your certificate expires, or use the application's Expiration Notification function (located in System LDAP > Certificates). Ensure that you have a new certificate ready before the old one expires. This gives you time to install and test the new certificate before the old one expires.
Set up a stand-alone certificate authority for active directory
The first step to configure Microsoft Active Directory for SSL access is to set up a stand-alone Certificate Authority (CA).

Role required: admin

Do not worry about addition resource utilization because both of the required services (IIS & CA) can be disabled after issuing the certificate(s).

1. Install Internet Information Server (IIS).
2. Install Certificate Authority Services in stand-alone mode.
3. Verify the Certificate Services web application is installed and active.

Using the IIS Manager console, expand the local computer and select Web Sites. The state of Default Web Site should be Running. You should also see a CertSvc application listed under the Default Web Site. If the site is not running or the application is missing, you must resolve the issue before you proceed.

Generate a certificate from an internal certificate authority
When you configure Microsoft Active Directory for SSL access, you must generate an internal certificate and request the external certificate.

Role required: admin

These steps apply to Microsoft CA services. If you have a different internal CA platform, see your local CA administrator for assistance.

1. From the domain controller (DC) you want to create a certificate for, browse to http://localhost/certsrv or specify the CA server name if it is on a remote server.
2. From the Welcome page, click Request a certificate and select advanced certificate request.
3. On the Advanced Certificate Request page, select Create and submit a request to this CA.
4. Complete the Advanced Certificate Request as follows:

<table>
<thead>
<tr>
<th>Advanced Certificate Request fields</th>
<th>Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The fully qualified domain name (FQDN) of the DC that is requesting the certificate.</td>
</tr>
<tr>
<td>E-Mail</td>
<td>The email address of the person responsible for the certificate.</td>
</tr>
<tr>
<td>Company</td>
<td>Your company name.</td>
</tr>
<tr>
<td>Key Options settings</td>
<td></td>
</tr>
<tr>
<td>Create new key set</td>
<td>Select it.</td>
</tr>
<tr>
<td>CSR</td>
<td>Microsoft RSA SChannel Cryptographic Provider.</td>
</tr>
<tr>
<td>Key Usage</td>
<td>Exchange.</td>
</tr>
<tr>
<td>Key Size</td>
<td>1024 is recommended. The instance supports up to 2048.</td>
</tr>
<tr>
<td>Automatic key container name</td>
<td>Select it.</td>
</tr>
<tr>
<td>Store certificate in the local computer certificate store</td>
<td>Select it.</td>
</tr>
</tbody>
</table>

5. Click Submit.
You are directed to a page that provides your Request ID, make note of this ID.
6. To process the pending request, complete the following:
   a) Open the Certificate Authority management console.
   b) Expand the server node and select Pending Requests.
   c) Locate the Request ID for the request you just submitted, right-click, and select All Tasks/Issue to approve the request and issue the certificate.

7. To retrieve the issued certificate, complete the following:
   a) From the DC you made the request from, browse to http://localhost/certsrv, or specify the CA server name if it is on a remote server.
   b) Select View the status of a pending certificate request.
   c) Select the link to the new certificate.
   d) Select the link to Install this certificate.

You need to request a third party certificate. Certificates from external CAs can be purchased for as little as $30 per year. For detailed procedures on requesting a certificate from an external CA, see Microsoft article 321051. After it is received, installed, and tested, follow the export procedure.

Test the LDAPS Connectivity Locally
When you configure Microsoft Active Directory for SSL access, you must test the LDAPS connectivity after installing the internal and third party certificates.

Role required: admin

1. Ensure that Windows Support Tools are installed on the domain controller (DC).
   The Support Tools setup (suptools.msi) can be found in the \Support\Tools directory on your Windows Server CD.
2. Select Start > All Programs > Windows Support Tools > Command Prompt. On the command line, type ldp to start the tool.
3. From the ldp window, select Connection > Connect and supply the local FQDN and port number (636). Also select the SSL.
   If successful, a window displays and lists information related to the Active Directory SSL connection. If the connection is unsuccessful, try restarting your system and repeat this procedure.

Export the public key certificate to trust the LDAP certificate
When you configure Microsoft Active Directory for SSL access, you must export the public key certificate and import it into the application.

Role required: admin

If your Certificate Authority is not a trusted third party vendor, you must export the certificate for the issuing CA so we can trust it, and, by association, trust the LDAP server certificate. For MS Certificate Services users, you can view the certificate path by viewing the certificate in the console used to export; select the Certificate Path tab. You must export all certificates in the chain. You can find the CA certificate in the same folder as the LDAP certificate by looking for the name in the Certificate Path. Submit all certificates for importing to your instance.

1. From a current or new MMC console, add the Certificate (Local Computer) snap-in.
2. Open the Personal/Certificates folder.
3. Locate the new certificate. The Issued To column shows the FQDN of the domain controller.
4. Right-click the certificate and select All Tasks/Export.
5. Export to DER or Base-64 format. Name the file using the format: MyCompany.cer.
   This is the public key certificate the needs to be used on the instance to communicate securely with your domain controller.
6. Test LDAPS locally before you submit the certificate to the instance.

After completing this procedure, import the public key certificate into the application.

See Install the LDAP X.509 SSL certificate to upload the certificate into the application.

**LDAP global catalog usage**

A DC can be granted the Global Catalog (GC) role. Global Catalog (GC) role is an LDAP-compliant directory consisting of a partial representation of every object from every domain within a forest.

Administrators configure Active Directory to host Lightweight Directory Access Protocol (LDAP) directory information using one of the following hosting methods.

- The common method of hosting LDAP directory information is to use the default LDAP or LDAPS (secure LDAP) on ports 389 or 636. These standard LDAP ports always exist on a Domain Controller (DC) and are rarely changed. Accessing this directory partition provides access to all of the objects within the domain that is hosted on the DC. There is no way to access objects from other domains using this method.

- A DC can also be granted the Global Catalog (GC) role. Global Catalog (GC) role is an LDAP-compliant directory consisting of a partial representation of every object from every domain within the forest. This LDAP directory can be accessed on port 3268, with LDAPS on port 3269. LDAPS and the default LDAP ports' certificate requirements are the same.

**Global Catalog LDAP dependencies**

- The domain controller that your instance connects to must have the Global Catalog role enabled.
- Firewall rules must allow inbound traffic to the domain controller on port 3268 (LDAP) or 3269 (LDAPS).

**Special notes**

- Not all attributes are replicated to the GC partition. Common attributes such as first name, last name, email, phone number, description, and address are included. Additional attributes can be added to the GC but should be limited to minimize the impact to forest replication traffic.
- Standard LDAP integrations usually use sAMAccountName as the instance's UserID and as the coalesce key in the LDAP import map since this is guaranteed to be unique within a domain. This attribute is no longer unique when viewing an entire forest of domains. A new unique attribute needs to be identified and as the UserID and the coalesce key. These do not need to be the same attribute and may vary based on your forest design. Consult your Active Directory administrator. Typically, the userPrincipalName is a unique attribute across domains but this may not be a user-friendly name to login with, but it could be used for the unique identifier on imports. A common attribute that is used for the UserID is email address. These decisions impact the LDAP Properties and LDAP Mapping.
- The value used for the coalesce key on the LDAP import map must be unique and exist on every object being imported. If it is not unique or does not exist, incorrect records are updated with changes.
- If you already have an LDAP integration and wish to change it to a GC, change the import coalesce key. The new key values must be imported before you can change the coalesce key.
- If you make any changes to your LDAP integration that break your integration, your first step should be to revert those changes. After that, contact Customer Service and Support with complete information about what you're attempting.

**OpenLDAP minor schema modification**

In OpenLDAP 2.3 systems that use the back-bdb (Berkley backend), administrators make a minor modification to their schema to facilitate the integration.
CAUTION: The customization described here was developed for use in specific instances, and is not supported by ServiceNow Technical Support. This method is provided as-is and should be tested thoroughly before implementation. Post all questions and comments regarding this customization to our community forum.

In OpenLDAP 2.3, back-bdb has limited support for inequality indexing (ordering). It is implemented only for generalizedTime and ChangeSequenceNumber syntax. It cannot be supported on syntax that support substrings. Search filters containing inequalities are processed using the presence index.

We recommend creating a custom attribute for this purpose, instead of changing what is already indexed or present in the schema (for example, `servnowid`).

Modify the OpenLDAP schema
These steps detail a schema modification to OpenLDAP 2.3 provided by one of our customers that helped them integrate with their instance.

Role required: admin

CAUTION: The customization described here was developed for use in specific instances, and is not supported by ServiceNow Technical Support. This method is provided as-is and should be tested thoroughly before implementation. Post all questions and comments regarding this customization to our community forum.

To modify the OpenLDAP schema for integration with the instance:

1. Create a custom attribute.

```plaintext
attribute ( 1.3.6.1.4.1.3403000.2.1.8
    NAME 'servnowid'
    ORDERING caseIgnoreOrderingMatch
    EQUALITY caseIgnoreMatch
    SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

2. Include the attribute in the selected objectclass OID.

```plaintext
objectclass ( 1.3.6.1.4.1.3403000.2.2.1
    NAME 'BcfUserIdentifiers' SUP top AUXILIARY
    MAY ( uniqid $ unixid $ servnowid ) )
```

In OpenLDAP 2.3, you can dynamically change the server configurations, but you can only extend the schema. You cannot modify or delete the existing schema. Instead of creating another objectclass for this attribute in the dynamic configuration, use the static configuration file, slapd.conf.

3. In slapd.conf, include indexing for the new attribute in the bdb section of your main database backend.

```plaintext
database bdb (configs here) ....
    index servnowid pres
    (other indexes here) .....  
```

4. As root, run slapindex to index this attribute to make it available in search filters. Make sure that the OpenLDAP daemon is not running or is in read-only mode before starting slapindex.

Record LDAP deletions
By default, the instance does not delete any entries after they disappear from LDAP.

Deleting an entry, also referred to as a record, also deletes the entire history and references to the deleted entry.
For example, configuration items (CIs), SLA agreements, software licenses, purchase orders, and service catalog entries all have a reference to Department, and if a department is deleted, then the integration clears all references to the department. Also, deleting a user results in losing all history of what that user did.

Decide whether to retain or manually delete records according to your organization's needs.

**Adaptive authentication**

Adaptive authentication is a policy framework that allows enforcement of contextual authentication controls to the right persona at the right time. Adaptive authentication uses authentication policies to evaluate authentication requests and then either deny or allow access based on the specified policy conditions.

You can use the authentication policies to restrict access of users and APIs based on various criteria like IP address, user role, and user group. You can configure the built-in authentication policies according to your security requirements.

For example, an administrator can configure the Allow Access Policy to allow users only from a trusted range of IP addresses and users of a specific role. The configured access policy denies access from untrusted IP addresses.
REST API access policies

You can use the filter criteria of Adaptive Authentication framework to restrict access to inbound ServiceNow REST APIs. For more information, see REST API access policies.

Activate adaptive authentication

You can activate the Adaptive Authentication plugin (com.snc.adaptive_authentication) for Adaptive Authentication if you have the admin role.

Role required: admin

1. Navigate to System Applications > All Available Applications > All.
2. Find the Adaptive Authentication plugin (com.snc.adaptive_authentication) using the filter criteria and search bar.
   You can search for the plugin by its name or ID. If you cannot find a plugin, you might have to request it from ServiceNow personnel. For more information, see Request a plugin.
3. Click Install, and then in the Activate Plugin dialog box, click Activate.

   Note: When domain separation and delegated admin are enabled in an instance, the administrative user must be in the global domain. Otherwise, the following error appears: Application installation is unavailable because another operation is running: Plugin Activation for <plugin name>.

Filter criteria

Filter criteria (Policy Inputs) are used as inputs for policy conditions to verify and meet the requirements of an authentication request. For example, an IP Filter Criteria defines an IP address in the Subnet (Classless Inter-Domain Routing - CIDR format) or a range of IP addresses.

You can create filter criteria based on the user's IP address, role, and the user group to which they belong. Filter criteria is also called as policy inputs.

Create IP filter criteria
IP filter criteria allows you to filter users based on the user's IP addresses. You can configure an authentication policy to allow or deny access to a specific address or range of addresses.

Role required: admin

2. Click New.
3. On the form, fill in these fields.
4. Right-click the form header and click **Save**.

5. From the **IP Range** tab, double-click **Insert a new row**.

You can enter a single IP address or multiple ranges of IP addresses. For example, for a range of IP addresses enter `192.0.2.0` in the **Start IP** column and `192.0.2.255` in the **End IP** column.

![IP Filter Criteria form](image)

**Note:** For a single IP addresses, make sure that you enter the same IP address in the **Start IP** address and **End IP** columns. When you enter an IP address in the **Start IP** column, leave the **End IP** column blank and then save the record. The **End IP** column is auto-populated with the same **Start IP** address.
6. From the **Subnet (CIDR)** tab, double-click **Insert a new row**.
Enter the Network IP address and Netmask in the Classless Inter-Domain Routing (CIDR) format. For example, enter `255.255.255.0` as Network IP and `25` as Netmask.

<table>
<thead>
<tr>
<th>IP Range</th>
<th>Subnet (CIDR)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Network IP</td>
</tr>
<tr>
<td></td>
<td>255.255.255.0</td>
</tr>
<tr>
<td></td>
<td>Netmask</td>
</tr>
<tr>
<td></td>
<td>25</td>
</tr>
</tbody>
</table>

**Create role filter criteria**
Role filter criteria allows you to filter users based on the roles. You can configure an authentication policy to allow or deny access to a list of user roles.

Role required: admin

1. Navigate to **Adaptive Authentication > Filter Criteria > Role Filter Criteria**.
2. Click **New**.
3. On the form, fill in these fields.

<table>
<thead>
<tr>
<th><strong>Role Filter Criteria form</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Application</td>
</tr>
<tr>
<td>Description</td>
</tr>
</tbody>
</table>

4. From the **Roles for criteria**, double-click **Insert a new row**.
5. Create a condition for a specific role using the Condition Builder. For example, you can create a condition that allows only users with admin, itil, or snc_internal roles. For more information about Condition Builder, see Create a condition statement using the condition builder.

**Note:** Currently, Dot-walking is not supported in Role filter criteria.

<table>
<thead>
<tr>
<th>Name</th>
<th>Admins only</th>
<th>Application</th>
<th>Global</th>
</tr>
</thead>
</table>

Condition builder example:

- Role is admin
- Role is itil
- Role is snc_internal

---

Create group filter criteria

Group filter criteria allows or denies user access based on the user group to which the user belongs.

Role required: admin

2. Click New.
3. On the form, fill in these fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name to identify the group.</td>
</tr>
<tr>
<td>Description</td>
<td>Short description of the group.</td>
</tr>
<tr>
<td>Application</td>
<td>Scope of the application.</td>
</tr>
</tbody>
</table>

4. From the Groups for criteria tab, double-click Insert a new row.
5. Click the search icon
   ![Search Icon]
   look up, and select a user group.

6. Click the save icon
   ![Save Icon]

**Authentication policies**

Authentication policies evaluate authentication requests based on the specified policy conditions and either allow or deny access depending on the output of policy conditions evaluation. For example, access is allowed only if all the policy conditions specified in Allow Access Policy evaluate to true.

You can use the built-in authentication policies or create an authentication policy according to your security requirements.

**Note:** At any point of time, either Allow Access Policy or Deny Access Policy can be executed but not both.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Access Policy</td>
<td>Denies all the authentication requests by default. Allows only the authentication requests that match the specified policy conditions.</td>
</tr>
<tr>
<td>Deny Access Policy</td>
<td>Allows the authentication requests by default. Denies only the authentication requests that match the specified policy conditions.</td>
</tr>
<tr>
<td>Global Blocking Policy</td>
<td>Denies the access requests of users and APIs before authentication. This policy can be used as an alternative to the IP Address Access Control.</td>
</tr>
</tbody>
</table>

**Configure allow access policy**

Allow access policy denies all the authentication requests by default. Allows only the authentication requests that match the specified policy conditions.

Role required: admin

2. From the Policy Inputs tab, click Edit.
3. Select one or more filter criteria from the **Collection** list and move them to **Policy Inputs List** of **Allow Access Policy** list.

4. From the **Policy Conditions** tab, click **New**.

   **Note:** When there are multiple policy conditions, the final output of the access policy depends on the logical OR output of all policy conditions.

5. On the form, fill in the fields:

   **Condition form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>Name to identify the condition.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the condition.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Condition</td>
<td>Logical combination of multiple policy inputs(filter criteria) that is used to evaluate authentication requests. For example, you can create conditions that allow only contractors from a list of trusted IP addresses.</td>
</tr>
</tbody>
</table>

**Configure deny access policy**

Deny access policy allows all the authentication requests by default. Denies only the authentication requests that match the specified policy conditions.

Role required: admin

1. Navigate to **Adaptive Authentication > Authentication Policies > Deny Access Policy**.
2. From the **Policy Inputs** tab, click **Edit**.
3. Select one or more filter criteria from the **Collection** list and move them to **Policy Inputs List** of **Deny Access Policy** list.
4. From the **Policy Conditions** tab, click **New**.

**Note:** When there are multiple policy conditions, the final output of the access policy depends on the logical OR output of the all policy conditions.

5. On the form, fill in the fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>Name to identify the condition.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the condition.</td>
</tr>
<tr>
<td>Condition</td>
<td>Logical combination of multiple policy inputs(filter criteria) that is used to evaluate authentication requests. For example, you can create conditions that deny access to employees from a range of untrusted IP addresses.</td>
</tr>
</tbody>
</table>

**Configure global blocking policy**

Global blocking policy denies the authentication requests of users and APIs based on the specified policy conditions. This policy can be used as an alternative to the IP Address Access Control.

Role required: admin

1. Navigate to **Adaptive Authentication > Pre-Authentication Policies > Global Blocking Policy**.
2. From the **Policy Inputs** tab, click **Edit**.
3. Select one or more IP filter criteria from the Collection list and move them to Global Blocking Policy list.

**Note:** Global blocking policy supports only IP Filter criteria.

4. From the Policy Conditions tab, click New.

**Note:** When there are multiple policy conditions, the final output of the access policy depends on the logical OR output of the all policy conditions.

5. On the form, fill these fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>Name to identify the condition.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the condition.</td>
</tr>
</tbody>
</table>
Configure adaptive authentication properties

After activating the Adaptive Authentication, configure adaptive authentication properties according to your security requirements.

Role required: admin

2. Configure these properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Authentication Policy</td>
<td>Option to enable the authentication policy.</td>
</tr>
</tbody>
</table>
## Property Description

Execute Deny Access Policy by default and access is denied only if conditions defined in deny access policy evaluates to true

This property is selected by default when you activate the Adaptive Authentication plugin. When you select the **Enable Authentication Policy** property, Deny Access Policy is executed by default and all users are allowed access. Access is denied only when the specified Deny Access Policy conditions evaluate to true.

When you clear this property, Allow Access Policy is executed by default. Allow Access Policy allows users only when the specified Allow Access Policy conditions evaluate to true.

**Note:** Before you clear this property, make sure that Allow Access Policy is configured accurately. Otherwise, Allow Access Policy denies access to the users who do not match the specified policy conditions.

For example, an administrator configures Allow Access Policy to allow only employees from the IP range of 192.0.2.0 to 192.0.2.24 and Deny Access Policy to deny access for the contractors.

**Note:** At any point of time, either Allow Access Policy or Deny Access Policy can be executed but not both.

When an administrator selects the **Enable Authentication Policy** property as 'Yes' and sets the **Execute Deny Access Policy by default and access is denied only if conditions defined in deny access policy evaluates to true** property as 'No', only employees from the IP range of 192.0.2.0 to 192.0.2.24 are allowed. Rest of the employees from other IP addresses are denied access, even though they have valid credentials.

Enable debug logging for authentication policies

Option to enable debug logging for the authentication policies.

HTTP error code to be displayed to the user when access is blocked by Global Blocking Policy

HTTP error code that displays during login when the Global Blocking Policy blocks a user login.

Error message to be displayed to the user when access is blocked by Global Blocking Policy (only applicable when Forbidden(403) HTTP error code is selected)

Error message that displays when the Global Blocking Policy blocks access.

### Authentication with SAML

The Security Assertion Markup Language (SAML) is an XML-based standard for exchanging authentication and authorization data between security domains.

SAML exchanges security information between an identity provider (a producer of assertions) and a service provider (a consumer of assertions). SAML is a product of the OASIS Security Services Technical Committee. When implemented correctly, SAML is one of the most secure methods of single sign-on (SSO) available.
The SAML 2.0 integration enables SSO by exchanging XML tokens with an external Identity Provider (IdP). The IdP authenticates the user and passes a NameID token to the system. If the system finds a user with a matching NameID token (for example, the email address), the instance logs that user in.

If you are using the SAML 2.0 plugin for SSO authentication, you need to set the glide.ui.rotate_sessions property to false. Otherwise, it interferes with the session information sharing that takes place between the instance and the Identity Provider. Users with the security_admin elevated privilege can access this property.

**Note:** It is recommended that customers using an existing SAML 2.0 integration upgrade to the Multi-Provider SSO plugin.

To learn more about the properties that affect SAML 2.0 processing, see SAML 2.0 web browser SSO profile SAML 2.0 web browser SSO profile (instance security hardening).

### Activate and set up SAML 2.0

SAML 2.0 activates through the Integration - Multiple Provider Single Sign-On Installer plugin.

**Note:**

Activate the Integration - Multiple Provider Single Sign-On Installer plugin to set up SAML 2.0 authentication. Refer to this plugin when directed to find and click the plugin name.

1. Navigate to **System Applications > All Available Applications > All.**
2. Find the plugin using the filter criteria and search bar.

   You can search for the plugin by its name or ID. If you cannot find a plugin, you might have to request it from ServiceNow personnel. For more information, see [Request a plugin](#).
3. Click **Install**, and then in the Activate Plugin dialog box, click **Activate**.

**Note:** When domain separation and delegated admin are enabled in an instance, the administrative user must be in the global domain. Otherwise, the following error appears: Application installation is unavailable because another operation is running: Plugin Activation for <plugin name>.

### Clone an instance with a SAML integration

Before cloning an instance that uses SAML 2.0, preserve the SAML SSO-related settings on the target instance. Failing to do so might make the target instance inaccessible.

Role required: admin

1. On the source instance, navigate to **System Clone > Preserve Data > Core Instance Properties.**
2. Make sure that the following SAML SSO-related properties are preserved using conditions, as shown:

- glide.authenticate
- glide.security
- glide.entry
- glide.script
- glide.session
- glide.saml2
- com.glide.communications
- com.snc.integration.saml_esig
3. On the source instance, navigate to **System Clone > Preserve Data** to preserve SAML certificates on sys_certificate and SAML users on sys_user related to SAML/SSO/Multi SSO. If you need them, export them into XML, then manually import them on the target.

**Warning:** Do not try to clone the SAML/SSO/Multi SSO setup from one system to another. Most transfers of SAML/SSO or Multi SSO settings do NOT work because they must be configured on the identity provider. If you overwrite a working setup, the target instance will fail to authenticate so your target instance will become inaccessible. Also, do not change the sys_id of your Multi SSO provider record; doing that will force your users to flush their cookies. For more information about cloning precautions, see Checklist before cloning an instance.

4. Exclude the Multi SSO tables sso_properties, digest_properties and saml2_update1_properties.

5. Manually create the SAML/SSO/Multi SSO records on each instance independently and set up the records on your identity provider as well.

6. Make sure that you manually create a LOCAL admin account on sys_user (not in LDAP or SAML) record on the target instance and with a sys_id that does not exist on the source instance.

7. Click **Update**.

**Identity Provider (IdP) system properties**

An IdP generally offers an XML document containing their authentication and logout metadata.

For example, SSOCircle publishes their metadata online.

Browse the IdP metadata to find these entries:

- The **SingleSignOnService** element with a **Binding** attribute that contains a value of **HTTP-Redirect**. The **Location** attribute lists the URL the integration requires for the AuthnRequest service.
- The **SingleLogoutService** element with a **Binding** attribute that contains a value of **HTTP-Redirect**. The **Location** attribute lists the URL the integration requires for the SingleLogoutRequest service.

**Note:** The SAML 2.0 integration only supports binding to IdP services by HTTP-Redirect.

For example:

```
```

```
```
IdP properties

Set the IdP issuer URL

Provide the URL to the IdP's who will issue the security token.

Role required: admin

The integration verifies that each SAML response contains the same URL listed in this system property as the URL listed in the `Issuer` element. For example:

```
<snmp:Response xmlns:snmp="urn:oasis:names:tc:SAML:2.0:protocol"
   Destination="https://demo12.service-now.com/navpage.do"
   ID="s28da6774c88ae1a292bf25fe625db81919d8e1e"
   InResponseTo="SNC841720c227c81948cf68cadcad235c6"
   IssueInstant="2012-01-30T20:07:10Z" Version="2.0"><snmp:Issuer
   ...
   <snmp:Assertion xmlns:snmp="urn:oasis:names:tc:SAML:2.0:assertion"
      ID="s2f347f973c63836cf70ea38302d94976f9c5b851"
   ...
</saml:Assertion></snmp:Response>
```

1. Navigate to SAML 2 Single Sign-on > Properties.
2. In the property **The Identity Provider URL which will issue the SAML2 security token with user info.**, enter the URL to your IdP. Each IdP URL must be unique.

   By default, the integration contains the URL to SSOCircle http://idp.ssocircle.com.

Set the AuthnRequest service URL

   Using the IdP's metadata, set the request service URLs for the integration's IdP.

   Role required: admin

   1. In the property **The base URL to the Identity Provider's AuthnRequest service. The AuthnRequest will be posted to this URL as the SAMLRequest parameter**, enter the URL to the HTTP-Redirect binding obtained from the SingleSignOnService element.

   2. Select the check box next to **Sign AuthnRequest** to enable the Identity Provider's single-sign on service to receive a signed AuthnRequest.

   3. In the property **When SAML 2.0 single sign-on fails because the session is not authenticated, or this is the first login, redirect to this URL. This is the base URL where the initial SAML 2.0 AuthnRequest is sent using the SAMLRequest parameter**, enter the URL to the HTTP-Redirect binding obtained from the SingleSignOnService element.

   By default, the integration contains the URL to the SSOCircle service.

Set the SingleLogoutRequest service URL

   Using the IdP's metadata, set the request service URLs for the integration's IdP.

   Role required: admin

   1. In the property **The base URL to the Identity Provider's SingleLogoutRequest service. The LogoutRequest will be posted to this URL as the SAMLRequest parameter**, enter the URL obtained from the SingleLogoutService element.

   By default, the integration contains the URL to the SSOCircle service.

   2. In the property **URL to redirect users after logout, typically back to the portal that enabled the SSO (e.g. http://portal.companya.com/logout)**, enter the URL where you want to redirect users after they successfully logout. If your IdP uses form-based authentication, enter the URL to your IdP's login form. If your IdP uses a non-form-based authentication method such as Kerberos, you should set the URL to a static logout page. This way, users who log out do not get immediately get redirected to the IdP and login again.

   By default, the integration contains the URL to the static UI page external_logout_complete.do.

(Optional) Enable signed logout requests

   Some IdPs require the Service Provider to sign logout requests with a certificate.

   Role required: admin

   If your IdP requires signed logout requests, use the IdP's metadata to set the following system properties.

   1. From the property **Sign LogoutRequest. Set this property to true if the Identity Provider's SingleLogoutRequest service requires signed LogoutRequest**, select Yes to specify that your IdP requires a signed logout request, or select No to use unsigned logout requests.

   2. If you selected Yes to Sign LogoutRequest, then in The protocol binding for the Identity Provider's SingleLogoutRequest service. (Value can be either "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" or "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST") property, enter the one of the supported values listed in Binding attribute from the SingleLogoutService element.

   By default, the integration uses an HTTP-Redirect binding.

3. Click Update.

4. Install a Service Provider (SP) key store.
Service Provider (SP) system properties
These system properties define how the instance interacts with the IdP as a Service Provider.

Service Provider (SP) properties

The URL to the ServiceNow instance homepage.
https://yourinstance.servicenow.com/navpage.do

The entity identifier, or the issuer.
https://yourinstance.servicenow.com

The audience URI that accepts SAML2 token. (Normally, it is your instance URL. For example: https://demo.servicenow.com)
https://yourinstance.servicenow.com

The User table field to match with the Subject’s NameID element in the SAMLResponse

email

The NameID policy to use for returning the Subject’s NameID in the SAMLResponse. Your SAML identity provider will have to support this by declaring the policy in its metadata. The NameID value is used to match with the specified field in the User table to lookup the user.

urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

Create an AuthnContextClass request in the AuthnRequest statement. This tells the IdP that ServiceNow requires that they present a specific login mechanism such as a form, Kerberos, etc. If the AuthnRequest doesn’t specify an AuthnContextClass, the IdP will choose the most appropriate method.

Yes | No

The AuthnContextClassRef method that we will be included in our SAML 2.0 AuthnRequest to the Identity Provider

urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport

The alias of key entry stored in SAML 2.0 SP Keystore used to sign SAML 2 requests.

saml2sp

The password of key entry stored in SAML 2.0 SP Keystore used to sign SAML 2 requests.

********

Service Provider properties

Set the instance URL for SAML
Set the instance-specific URLs so the IdP can authenticate users.

Role required: admin

1. In the property **The URL to the Service-now instance (usually this instance)**, enter the URL (including login page) of the instance for which the IdP authenticates. For example: https://yourinstance.service-now.com/navpage.do

2. In the property **The entity identification, or the issuer**, enter the base URL (excluding login page) of the instance for which the IdP authenticates. For example: https://yourinstance.service-now.com/

Set the audience URL for SAML
The Audience system property allows your instance to verify that it is the intended recipient of a SAML response.

Role required: admin

The integration verifies that each SAML response contains the same URL listed in this system property as the URL listed in the **Audience** element. For example:

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
ID="s2cdcc74f37f923e26f1e4e4c42b0a9324230334f"
InResponseTo="90AA6073F01567BF80DF1945B96314E2" Version="2.0"
IssueInstant="2010-04-29T23:21:51Z" Destination="https://dloomac.service-
now.com/navpage.do">
...
<saml:Conditions NotBefore="2012-01-30T19:57:10Z"
demoi2.service-now.com</saml:Audience><saml:AudienceRestriction></saml:Audience></saml:Conditions>
...
</samlp:Response>
```

1. Navigate to **SAML 2 Single Sign-on > Properties**.
2. In the property **The audience uri that accepts SAML2 token. (Normally, it is your instance URL. For example: https://<instance name>.service-now.com.)**, enter the URL of your instance. For example, https://demoi2.service-now.com. This URL must match the value of the **Audience** element in the SAML Response.
3. Click **Update**.

Set up a NameID policy for SAML
SAML 2.0 requires the Idp to exchange a NameID token with the service provider.

Role required: admin

For the SAML 2.0 integration the NameID token must map to a particular field in the User table. The integration uses the NameID token’s value to determine what user the IdP authenticates.

1. Browse the IdP metadata to find the **NameIDFormat** element that contains a value of emailAddress. The value of this element is the default format that the integration uses.
2. Review other **NameIDFormat** elements to determine if there are formats that match other fields in the User table.

Determine what User table field matches the NameID token
Identity providers specify what format the NameID token has.

Role required: admin

Setting up SAML 2.0 requires selecting a field from the User table that matches the format of the NameID token. Typically, IdPs offer the option to use an email address as the NameID token. Since the User table contains an email field, this field is a logical choice for use as a NameID token. To use another field from the User table as the NameID
token, first verify that the IdP offers a NameID format that matches the value of a User table field. This may require adding the field to the User table.

1. Compare the available formats in the IdP's NameIDFormat element to fields in the User table.
2. Select a NameID format where there is a matching value in the User table.
3. In the The User table field to match with the Subject's NameID element in the SAMLResponse field, enter the name of the User table field to search for matching values in the NameID token.

By default, the integration uses the email field.

Set the IdP NameID policy
Specify what format the IdP uses for the NameID token.
Role required: admin
This format is listed as part of the IdP's metadata.

1. In the property The NameID policy to use for returning the Subject's NameID in the SAMLResponse. Your SAML identity provider will have to support this by declaring the policy in its metadata. The NameID value is used to match with the specified field in the User table to lookup the user., enter the value of the NameIDFormat element the integration uses.

By default, the integration uses the SSOCircle NameIDFormat for email addresses.
2. Click Save.

Values in the User table field for SAML
Ensure that the integration's User table field contains appropriate matching values.

For example, if the integration uses the email field as the NameID token, ensure that the instance lists the same email address as the IdP. The integration fails to authenticate any user who does not have a matching value for the NameID token.

(Optional) Enable providing an authentication context class for SAML
You can enable the instance to send an authentication context class request to the IdP containing your instance's preferred authentication request format.
Role required: admin
If you enable creating an AuthContextClass message, then you must also specify an authentication context class reference format.

Note: Some IdP's do not allow the Service Provider to set the authentication context class. Disabling this setting allows the IdP to choose the authentication context class.

1. From the property Create an AuthnContextClass request in the AuthnRequest statement, select Yes to specify a particular context class such as Password Protected Transport, or select No to have the IdP select the most appropriate context class.
2. If you selected Yes to Create an AuthnContextClass request in the AuthnRequest statement, then in The AuthnContextClassRef method that we will request in our SAML 2.0 AuthnRequest to the Identity Provider property, enter the URN of the context class you want to use for authentication (see table).

AuthnContextClass URN options

<table>
<thead>
<tr>
<th>Authentication type</th>
<th>Authentication context class URN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forms-based authentication</td>
<td>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</td>
</tr>
</tbody>
</table>
By default, the integration uses a Password Protected Transport authentication method.

3. Click **Update**.

(Optional) Set keystore properties for signing logout requests for SAML
The keystore properties allow the integration to sign logout requests using your signed server and signed CA certificates.

Role required: admin

1. In the property **The alias of key entry stored in SAML 2.0 SP Keystore used to sign SAML 2 requests**, enter the alias name you created for the SAML 2.0 Keystore. By default, the integration looks for the alias `saml2sp`.
2. In the property **The password of key entry stored in SAML 2.0 SP Keystore used to sign SAML 2 requests**, enter the password to your SAML 2.0 Keystore. By default, the password is the same as the default alias name.
3. Click **Update**.
4. Regenerate your SP metadata.

Install a service provider keystore for signing SAML requests
Use the following steps to remove the existing example key store and install your own Service Provider key store containing your public and private key pair.

Role required: admin

1. Create a Service Provider key store.
2. Navigate to **SAML 2 Single Sign-on > Certificate**.
3. Click **SAML 2.0 SP Keystore**.
4. Click the Manage Attachments link.
5. Select the Delete checkbox next to `saml2sp_keystore`.
6. Click **Remove**.
7. Click **Choose Files** and select the Keystore containing your signed certificates.
8. Click **Attach**.
9. Close the Attachments popup.
10. In **Key store password**, enter the password to access the SAML 2 alias.
11. Click **Update**.

Create a service provider keystore for SAML
In order for your instance to sign logout requests, you must create a Java Key store containing the following items.

- Signed server certificate for the instance
- Signed CA certificate
- Public and private key pair

You may create your own signed certificate with a private certificate authority or purchase one from a public certificate authority.

The following steps illustrate how to generate a new Java Keytool keystore file, create a certificate signing request (CSR), and import certificates. Any root or intermediate certificates need to be imported before importing the primary certificate for your domain. Type these commands in a command line interface.
Note: These instructions are not specific to the platform and require technical knowledge of security certificates to complete. Technical Support cannot assist in creating the certificates.

1. Generate a Java keystore and key pair.
   
   ```bash
   keytool -genkey -alias mydomain -keyalg RSA -keystore my.keystore
   ```

2. Generate a CSR for an existing Java keystore.
   
   ```bash
   keytool -certreq -alias mydomain -keystore my.keystore -file mydomain.csr
   ```

3. Import a root or intermediate certificate authority CA certificate to an existing Java keystore.
   
   ```bash
   keytool -import -trustcacerts -alias root -file Thawte.crt -keystore my.keystore
   ```

4. Import a signed primary certificate to an existing Java keystore.
   
   ```bash
   keytool -import -trustcacerts -alias mydomain -file mydomain.crt -keystore my.keystore
   ```

(Optional) Advanced SAML properties

The following advanced settings allow you to further increase security and debug the integration.

Advanced settings

<table>
<thead>
<tr>
<th>Advanced settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The number in seconds before &quot;notBefore&quot; constraint, or after &quot;notOnOrAfter&quot; constraint, to consider still valid.</td>
<td>60</td>
</tr>
<tr>
<td>Turn on debug logging for SAML 2.0 Authentication</td>
<td>Select Yes to enable additional logging information for SAML 2.0 events.</td>
</tr>
</tbody>
</table>

Advanced system properties table

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The number of seconds &quot;notBefore&quot; constraint, or after &quot;notOnOrAfter&quot; constraint, to consider still valid</td>
<td>Enter the number of seconds to add to the NotBefore and NotOnOrAfter constraints to account for time differences between the IdP clock and SP clock. These constraints prevent against replay attacks by denying requests that are not made within the specified time frame. If the IdP clock and SP clock are significantly different, network latency may result in the SAML request being unauthorized. This property adds a grace period during which SAML requests and responses are still considered valid.</td>
</tr>
<tr>
<td>Turn on debug logging for SAML 2.0 Authentication</td>
<td>Select Yes to enable additional logging information for SAML 2.0 events.</td>
</tr>
</tbody>
</table>
Install the identity provider certificate
You can paste a PEM certificate into a X.509 Certificate form so the identity provider can verify communications with the service provider.

Role required: admin

The IdP’s certificate is located within the IdP’s metadata. The IdP developer determines where the certificate metadata resides when creating the local IdP.

Note: Certificates for single-sign on should always be in PEM format to work with SAML certificates.

1. Navigate to SAML Single Sign-on > Certificate.
2. Fill in the form fields (see table).
3. Click **Save**.
<table>
<thead>
<tr>
<th>Name</th>
<th>SAH, 2.0</th>
<th>Format</th>
<th>PEM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expiration notification</td>
<td>Enabled</td>
<td>Type</td>
<td>Trust Store Cert</td>
</tr>
<tr>
<td>Notify on expiration</td>
<td>System Administrator</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warn in days to expire</td>
<td>20</td>
<td>Expires</td>
<td>2016-08-17 12:57:21</td>
</tr>
<tr>
<td>Active</td>
<td>Yes</td>
<td>Expires in days</td>
<td>1,837</td>
</tr>
<tr>
<td>Short description</td>
<td>idp.soaricle.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Issuer</td>
<td>CN=CA, O=SOARIClC, C=DE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subject</td>
<td>CN=idp.soaricle.com, OU=Idp, O=SOARIClC, C=DE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PEM Certificate</td>
<td>BEGIN CERTIFICATE-----</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
**Note:** The integration does not currently sign the certificate in communications between the instance and the IdP.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The certificate name. Do not change the Name entry. The name of the X.509 certificate must be <strong>SAML 2.0</strong> in order for the integration to use it. This requirement is only true if you are not using External single sign-on (SSO).</td>
</tr>
<tr>
<td>Expiration notification</td>
<td>Select this option to send a notification to the users selected in the Notify on expiration field. By default, this is enabled.</td>
</tr>
<tr>
<td>Notify on expiration</td>
<td>Select the users to revive the notification regarding certificate expiration. If no users are selected, the logged in user is added by default, along with the last two logged in users with the administrator role.</td>
</tr>
<tr>
<td>Warn in days to expire</td>
<td>The number of days before expiration that the instance send the notification. Enter a value of at least 20. Instances upgraded to Istanbul and later releases have this value set to 20 unless a greater value is specified.</td>
</tr>
<tr>
<td>Active</td>
<td>A check box to indicate that this certificate is active.</td>
</tr>
<tr>
<td>Format</td>
<td>The format of the certificate. SAML uses the <strong>PEM</strong> format.</td>
</tr>
<tr>
<td>Type</td>
<td>The certificate container. The instance recognizes certificates from trust stores, Java keystore, and PKCS#12 keystores.</td>
</tr>
<tr>
<td>Valid from</td>
<td>The instance automatically adds the certificate valid from date to this field. Attach the certificate to the X.509 certificate record to populate this field.</td>
</tr>
<tr>
<td>Expires</td>
<td>The instance automatically adds the certificate expiration date to this field. Attach the certificate to the X.509 certificate record to populate this field.</td>
</tr>
<tr>
<td>Expires in days</td>
<td>The calculated number of days to expiration.</td>
</tr>
<tr>
<td>Short description</td>
<td>A description for the certificate.</td>
</tr>
<tr>
<td>Issue</td>
<td>The instance automatically adds the certificate issuer to this field. Attach the certificate to the X.509 certificate record to populate this field.</td>
</tr>
<tr>
<td>Subject</td>
<td>The instance automatically adds the certificate subject to this field. Attach the certificate to the X.509 certificate record to populate this field.</td>
</tr>
<tr>
<td>PEM Certificate</td>
<td>Enter the value of the X509 certificate.</td>
</tr>
</tbody>
</table>

Click **Validate Stores/Certificates** to test the trust store and certificate.

Replacing a missing certificate for SAML
If the **Certificate** module displays a blank page, the SAML 2.0 certificate record has been deleted. You can replace the missing certificate by manually creating a certificate record.

**Role required:** admin

1. Navigate to **System Definition > Certificates**.
2. Create a new record called **SAML 2.0**.

   **Important:** You MUST use this name. This requirement is only true if you are not using External single sign-on (SSO).

3. Click **SAML 2 Single Sign-on > Certificate**.
4. In the **PEM Certificate** field, enter the value of the `ds:X509Certificate` element from your IdP's metadata.
5. Click **Save**.

Add a Java keystore for SAML

You can add Java keystores to the SAML application if you want another repository for your SAML security certificates.

**Role required:** admin

By default, SAML 2 Single Sign-on provides a default keystore named **SAML 2.0 SP Keystore** which uses 1024 bits and is SHA1. This keystore is active by default. If you need to use a key with 2048 bit key and SHA256, you need to activate this certificate before you generate your metadata with the x509 certificate. You can add keystores as needed and specify which one to use by default with a property.

1. Navigate to **System Definition > Certificates**.
2. Fill in the fields on the form (see table).
3. Click **Submit**.

![X.509 Certificate form](image)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a descriptive name.</td>
</tr>
<tr>
<td>Active</td>
<td>Select <strong>Active</strong> to keep the key store available.</td>
</tr>
<tr>
<td>Short description</td>
<td>Enter a description for the key store.</td>
</tr>
<tr>
<td>Type</td>
<td>Select <strong>Java Key Store</strong>.</td>
</tr>
<tr>
<td>Key store password</td>
<td>Enter the password for the key store.</td>
</tr>
</tbody>
</table>

4. To set the default key store, navigate to **System Properties > All Properties** and find and open the following property: `glideauthenticate.sso.saml2.keystore`

The Value field shows a default Sys ID (b88267271b012000f1129141be071393). If you have a custom keystore, you need to update this value to the newly created SAML 2.0 Keystore value. You might also need to do this after an upgrade from an earlier release.

5. Paste the Sys ID of the key store record that you created into the **Value** field.

6. Click **Update**.

*Install a service provider keystore for signing SAML requests*

Use the following steps to remove the existing example key store and install your own Service Provider key store containing your public and private key pair.

Role required: admin

1. Create a Service Provider key store.
2. Navigate to SAML 2 Single Sign-on > Certificate.
3. Click SAML 2.0 SP Keystore.
4. Click the Manage Attachments link.
5. Select the Delete checkbox next to saml2sp_keystore.
6. Click Remove.
7. Click Choose Files and select the Keystore containing your signed certificates.
8. Click Attach.
9. Close the Attachments popup.
10. In Key store password, enter the password to access the SAML 2 alias.
11. Click Update.

Test the SAML integration
After completing all other setup tasks, test the integration.

Role required: admin

1. Log in to the instance as a user with the admin role.
3. In the property Enable external authentication, select Yes.

Note:
Enabling external authentication requires all users to use SAML 2.0 single sign-on. Thus, if anyone tries to access the application in an unauthenticated state, the instance automatically sends an authentication request to the (IdP) and redirects the user to the SAML IdP Authentication page.

4. Click Save.
5. Log out of the instance.
6. Browse to the instance URL. If the integration is functioning properly, the IdP should ask for the users credentials.

Multi-SSO (SAML 2.0) errors and fixes
A list of common errors and associated fixes for a Multi-SSO (SAML 2.0) setup and configuration.

<table>
<thead>
<tr>
<th>Error in instance logs</th>
<th>Test Connection Message</th>
<th>SAML property</th>
<th>Diagnosis</th>
<th>Fix</th>
</tr>
</thead>
</table>
| NotAfter: <Thu Jun 05 22:57:44 PDT 2014>                                                | Ensure that the IDP x509 certificate is present, valid, and active.                    | N/A           | The current certificate or the SAML assertion has expired.                                                                                  | • Sync the SNC clock with the SAML IdP server clock.  
  • Update the SAML 2.0 certificate record.                                                |
<p>| • Unable to locate SAML 2.0 certificate.                                                 | Ensure that the IDP x509 certificate is present, valid, and active                     | The PEM-formatted string should be entered into the PEM Certificate field.                                                                 | • Ensure that the correct PEM-formatted certificate is uploaded to the instance. |
| • Could not find a digital signature stored in the ServiceNow instance.                 | The SAML certificate does not exist. It might be inactive.                              |                |                                                                                                                                           |                                                                      |</p>
<table>
<thead>
<tr>
<th>Error in instance logs</th>
<th>Test Connection Message</th>
<th>SAML property</th>
<th>Diagnosis</th>
<th>Fix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificates do not match. Expect: <code>&lt;certStr&gt;</code>, actual: <code>&lt;inboundCert&gt;</code>.</td>
<td></td>
<td>N/A</td>
<td>The available certificate in SNC does not match the certificate in assertion. Causes include:</td>
<td>Confirm that the PEM-formatted string in the SAML 2.0 certificate record matches the X509 Certificate in the SAMLResponse for the user IdP.</td>
</tr>
<tr>
<td>Failure to check the validity of the certificate.</td>
<td></td>
<td>N/A</td>
<td>The current certificate might have expired.</td>
<td>Update the SAML 2.0 certificate record.</td>
</tr>
<tr>
<td>Failure to validate signature profile.</td>
<td></td>
<td>N/A</td>
<td>The assertion might be signed with a different certificate.</td>
<td>Check if the IdP has the same certificate as the SNC instance.</td>
</tr>
<tr>
<td>InResponseTo attribute in SubjectConfirmationData mismatch. Expect: <code>&lt;inResponseTo&gt;</code>, actual: <code>&lt;inResponseTo&gt;</code>.</td>
<td></td>
<td>N/A</td>
<td>This error appears if either of the following situations occurs:</td>
<td>The IdP admin should confirm that the expected SAMLResponse is being returned. This situation can be a load balancer or infrastructure issue.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• The IdP returns a SAMLResponse for a different SAMLRequest</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• A user bookmarks the URL with the SAMLRequest instead of just the instance URL.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• If a null value is expected, the response might be sent to a different node when the instance has multiple nodes.</td>
<td></td>
</tr>
<tr>
<td>SessionIndex value not found: <code>&lt;message&gt;...</code></td>
<td>SessionIndex</td>
<td>N/A</td>
<td>The <code>SessionIndex</code> is required in the SNC instance. The IdP returns it in the SAML response to authenticate successfully.</td>
<td>The IdP admin should confirm that the <code>SessionIndex</code> is defined in the SAMLResponse.</td>
</tr>
<tr>
<td>No valid SubjectConfirmation found.</td>
<td>Subject confirmation</td>
<td>N/A</td>
<td>Conditions could be missing due to an error on the IdP. The Status Code in the response would contain Responder instead of the expected Success.</td>
<td>Review SAMLResponse to determine if Conditions are included in the SAMLResponse.</td>
</tr>
<tr>
<td></td>
<td>validation failed</td>
<td></td>
<td></td>
<td>The valid subject confirmation data could be expired or not for the right audience.</td>
</tr>
<tr>
<td>Error in instance logs</td>
<td>Test Connection Message</td>
<td>SAML property</td>
<td>Diagnosis</td>
<td>Fix</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------</td>
<td>---------------</td>
<td>-----------</td>
<td>-----</td>
</tr>
<tr>
<td>Assertion audience mismatch. Expect: <code>&lt;propAudience&gt;</code>, actual: <code>&lt;audienceUri&gt;</code>.&lt;br&gt; <strong>or</strong>&lt;br&gt; AudienceRestriction validation failed. No matching audience found.</td>
<td>Ensure that the 'Audience URI' field is set correctly</td>
<td>The audience URI that accepts the SAML2 token. (Normally, it is your instance URI. For example: <a href="https://demo.service-now.com">https://demo.service-now.com</a>.)</td>
<td>The SNC instance configured audience URI must match the value in the IdP.</td>
<td>Locate <code>&lt;saml2:Audience&gt;</code> in the SAMLResponse in the logs and verify that the value matches the one on the instance.</td>
</tr>
<tr>
<td>Assertion issuer is invalid. Expect: <code>&lt;value on instance&gt;</code>, actual: <code>&lt;value returned by IdP&gt;</code></td>
<td>Assertion issuer is invalid.</td>
<td>The Identity Provider URL that issues the SAML2 security token with user info.</td>
<td>The IdP entity id (issuer) does not match the value defined in the SNC instance.</td>
<td>• Check if IdP or SP is not configured properly.&lt;br&gt;• Confirm that the SAML property (the Identity Provider URL that issues the SAML2 security token with user info) is set correctly.</td>
</tr>
<tr>
<td>Subject is valid in the future. Now: <code>&lt;now&gt;</code>, NotBefore: <code>&lt;notBefore&gt;</code>&lt;br&gt; <strong>or</strong>&lt;br&gt; Subject is expired. Now: <code>&lt;now&gt;</code>, NotOnOrAfter: <code>&lt;notOnOrAfter&gt;</code></td>
<td>Subject validation confirmation failed.</td>
<td>The number in seconds before notBefore constraint, or after notOnOrAfter constraint, to consider still valid.</td>
<td>The IdP clock is not synced with SP clock.</td>
<td>Update the SAML property <code>glide.authenticate.sso.saml2clockskew</code> to a larger value. The default is 180 seconds. Some cases require a setting of 300 or higher. You may also need to check the time on your IdP server.</td>
</tr>
<tr>
<td>Assertion is valid in the future, now: <code>&lt;now&gt;</code>, notBefore: <code>&lt;notBefore&gt;</code>&lt;br&gt; <strong>or</strong>&lt;br&gt; Assertion is expired, now: <code>&lt;now&gt;</code>, notOnOrAfter: <code>&lt;notOnOrAfter&gt;</code></td>
<td>Assertion is invalid.</td>
<td>The number in seconds before notBefore constraint, or after notOnOrAfter constraint, to consider still valid.</td>
<td>IdP clock is not synced with SP clock</td>
<td>Update the SAML property to a larger value. Default of 60 seconds. Some cases require a setting of 300 or higher. You may also need to check the time on your IdP server.</td>
</tr>
</tbody>
</table>
### Common login and IdP errors

<table>
<thead>
<tr>
<th>Error or Symptom</th>
<th>Diagnosis</th>
<th>Fix</th>
</tr>
</thead>
</table>
| Login requests generate an infinite loop between the system and the IdP when High Security is active. | • Typically the URL endpoint is an error page or logout page.  
• The logout_redirect.do might create this loop when you define glide.security.url.whitelist without adding the IdP host name to the property value. | Set (or create) the system property glide.authenticate.failed_redirect to redirect failed authentication requests to this URL. |

**Note:** To learn more about this property, see URL allow list for logout redirects (instance security hardening) in Instance Security Hardening Settings.

The token used to authenticate the user or the request is signed with the signature algorithm http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 which is not the expected signature algorithm http://www.w3.org/2000/09/xmldsig#rsa-sha1.

Check the Alert Context tab for event details.

Navigate to the Advanced tab of the Relying Party Trust configuration dialog and verify that the algorithm is set to SHA-1 and not SHA-256.

---

### Redirect single sign-on (SSO) logins

When SSO is enabled, you can redirect users to specific pages or direct users to login locally.

For example, if a user attempts to go to https://customerX.service-now.com, an internal company portal can display instead of the default login page. Or, when a user logs out of an application, the browser can redirect them to a specific internal page. You can set redirection properties within the instance to ensure that users see an SSO login page rather than the default login page.

**Note:** The following properties do not force SSO. The login.do page is still accessible and users can login to the system if they have a local password set.

###Redirection properties

When a user logs out, or if there is a failed attempt to sign on using SSO, you can define where the user is taken next, such as a main portal page or a knowledge base article with SSO login information. Use the following properties to specify the URLs. If one of these properties does not exist in your instance, you can create the property.

**glide.authenticate.failed_requirement_redirect**

URL to redirect users when they attempt to access a page that is private (for example, to view an incident) and do not provide SSO credentials. The property is typically set to a customer's login portal (for example, http://portal.companya.com/).

**glide.authenticate.failed_redirect**

URL to redirect users after a failed SSO attempt. You can redirect to a public knowledge article that describes the error and has helpful links (for example, http://portal.companya.com/error).
**glide.authenticate.external.logout_redirect**

URL to redirect users after logging out, typically back to the portal that enabled the single sign-on log in (for example, http://portal.companya.com/logout).

**glide.authentication.external.disable_local_login**

When set to true, requires SSO credentials for the main login page. Defaults to false. This property needs to be used in conjunction with the `glide.authenticate.failed_requirement_redirect` property.

The following table shows the relationship between the Installation Exit return values, the properties, and the expected behavior.

<table>
<thead>
<tr>
<th>Return value</th>
<th>Property</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>failed_missing_requirement</td>
<td>glide.authenticate.failed_requirement_redirect</td>
<td>When this value is returned, it indicates that the required SSO credentials are not present in the session. Login fails and the session is redirected to the URL specified by the property. This is usually the URL for the SSO provider where login is challenged and credentials are collected.</td>
</tr>
<tr>
<td>failed_authentication</td>
<td>glide.authenticate.failed_redirect</td>
<td>When this value is returned, it indicates that the supplied SSO credentials failed authentication, the user does not exist, or the user is locked out. Login fails and the session is redirected to the URL specified by the property. This is usually the URL for the SSO provider where login is challenged and credentials are collected.</td>
</tr>
<tr>
<td>&lt;user_id&gt;</td>
<td>N/A</td>
<td>Login authorized for the user specified by &lt;user_id&gt;. This value matches with the field name defined in the SSO property <code>glide.authenticate.header.value</code> (&quot;the instance’s field name to match against the incoming header&quot;)</td>
</tr>
</tbody>
</table>

### Restricting local login

As a security precaution, you should do more than rely on redirection properties to prohibit logging in locally. If a user should never log in locally and will always be authenticated by your internal single sign-on system, then a random password should be assigned to each user that is imported into the instance. The random password is most easily set at the time of the user import. If the user data is imported into your system through an import set, you can create an `onBefore` transform script using the following code.

```java
var r = new Packages. java. util. Random () ;
var str1 = Packages. java. lang. Long. toString (Packages. java. lang. Long. random()) ;
```

© 2021 ServiceNow, Inc. All rights reserved.
Math.abs(r.nextLong(), 36); var str2 = Packages.java.lang.Long.toString(Packages.java.lang.Math.abs(r.nextLong()), 36);

var newPass = str1 + str2;
target.user_password = newPass;

//password now set to a random string like this:
//qvm81zdrn7cwwylpvw94eebk
SAML 2.0 concepts

Familiarize yourself with these SAML concepts.

Typical SAML process flow (diagram)

A typical SSO logic flow involves looking for an active session, checking user credentials, and creating the necessary token.

SSO Standard

Login (AuthnRequest) process flow

SAML 2.0 specifies a Web Browser SSO Profile that involves exchanging information among an identity provider (IdP), a service provider (SP), and a principal (user) on a web browser.

The identity provider can be any SSO service offering SAML authentication services (for example SSOCircle). The service provider is always an instance. The message flow begins with a request for a secured resource at the service provider.
Request the target resource at the SP

The principal requests a target resource at the service provider:

https://instance.service-now.com/

The instance checks the request to see if the SAMLRequest and RelayState URL parameters are present. If they exist, the user has already validated with the IdP and can skip steps 2–6.

Issue AuthnRequest to Identity Provider

The instance constructs an AuthnRequest to be sent to the IdP using the SAMLRequest value. The instance also constructs and sends a RelayState URL parameter value.

The RelayState token is an opaque reference to state information maintained at the service provider. The value of the SAMLRequest parameter is the deflated and base64 encoded value of the <samlp:AuthnRequest> element:

```
```

The integration then URL-encodes the <samlp:AuthnRequest> element and sends it as the SAMLRequest URL parameter.

The SSO service processes the <samlp:AuthnRequest> element by URL-decoding, base64-decoding and inflating the request, in that order. It then performs a security check. If the user does not have a valid security context, the IdP identifies the user by prompting for login credentials. If the user is already logged in, the IdP simply responds with the SAMLResponse and RelayState URL parameters (see step 3).

Respond with an SAMLResponse and RelayState

After collecting the required login credentials, the SSO service validates the request and responds with a document containing an XHTML form:

```
<form method="post" action="https://instance.service-now.com/navpage.do" ...><input type="hidden" name="SAMLResponse" value="response ..." /><input type="hidden" name="RelayState" value="token ..." />
...<input type="submit" value="Submit" /></form>
```

The value of the RelayState parameter comes from this step. The value of the SAMLResponse parameter is the base64 encoding of the following <samlp:Response> element:

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
```
Validate SAMLResponse

The SAMLResponse value is base64 decoded and inflated to reveal the XML document in step 3. The login script extracts the XML value from the //Subject/NameID element and uses it to look up an existing user in the User table.

The login script also extracts the session ID from the //AuthnStatement/@SessionIndex element and stores it for the LogoutRequest.

Logout (LogoutRequest) process flow
During logout, the instance issues the SAML 2.0 LogoutRequest service call to the IdP.

This service logs the user out and then redirects back to the specified logout URL.
SAML 2 Logout

User Clicks the Logout Button

The user clicks the **Logout** button and the instance executes the logout script.
LogoutRequest issued

The logout script constructs a SAML 2.0 LogoutRequest and posts it to the preconfigured SingleLogoutRequest SAML 2.0 service at the IdP. The IdP deflates the request and then base64 encodes it. An example LogoutRequest looks like this:

```xml
<saml2p:LogoutRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
  ID="21B78E9C6C8ECF16F01E4A0F15AB2D46"
  IssueInstant="2010-04-28T21:36:11.230Z"  Version="2.0">
  <saml2:Issuer
  <saml2:NameID
    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
    Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
    NameQualifier="http://idp.ssocircle.com"
    SPNameQualifier="https://dloomac.service-now.com/navpage.do">david.loo@service-now.com</saml2:NameID>
  <saml2p:SessionIndex>s211b2f811485b2a1d2cc4db2b271933c286771104</saml2p:SessionIndex>
</saml2p:LogoutRequest>
```

User Logs Out

The user logs out of the IdP. The IdP redirects back to the instance, which in turns redirects back to the IdP since the user is not logged in.
URL information for an SSO provider

During a login challenge resulting from a URL link into the instance that requires an SSO session, the referring URL might need to be supplied to the SSO provider so that after authentication, the URL can be passed back to the instance and linked to the correct resource.

SSO Logic Flow w/ Target Redirect Feature

SSO Target Redirect
Installation exit return values have been enhanced to pass a URL instead of, or in addition to the URL defined by the properties. Usually, you would return a username or a predefined string value to control authorize or challenge the SSO session. The following examples show the extended behavior of passing a URL.

```
```

The example above passes the URL https://instance.service-now.com/nav_to.do?uri=incident.do?sys_id=12345 to the SSO provider in the form of a URL parameter named TARGET.

**Note:** It is assumed that the SSO provider will use that information in the TARGET parameter to redirect back to the instance when the user credentials have been collected and authentication passed.

A colon : demarcates the two return values and an encoded & (%26amp;) concatenates the URL defined in the property `glide.authenticate.failed_missing_requirement` and the TARGET parameter.

### SAML 2.0 Single Sign-On — Update 1

The **SAML 2.0 Single Sign-On - Update 1: security enhancements** plugin improves integration security by requiring additional checks against the SAMLResponse URL parameter.

The integration explicitly checks the SAML response for the proper Identity Provider (IdP) and intended audience URLs.

#### Additional SAML response validations

With Update 1, the integration validates these elements in the SAMLResponse.

- An **Issuer** element that matches the value listed in the issuer system property
- The **SubjectConfirmation** and **SubjectConfirmationData** elements with a **Recipient** attribute
- The **AudienceRestriction** and **Audience** elements that match the value listed in the audience system property

#### Support for Signed SingleLogoutRequest

With Update 1, the SAML 2.0 integration has the option to sign SingleLogoutRequest elements. Some IdPs, such as Microsoft ADFS, require a signed SingleLogoutRequest.

#### Support for AuthnContextClass

With Update 1, the SAML 2.0 integration has the option to specify the method by which the IdP authenticates the user in the AuthnContextClass element. For example, the integration can now specify contexts such as form-based Password Protected Transport or Kerberos. See [Optional] Enable Providing an Authentication Context Class for instructions on setting an authentication context class.

#### No support for mobile iOS and Android apps

You cannot use the SAML 2 Update 1 plugin or the single sign-on (SSO) configuration provided by Okta for the iOS and Android apps. You must use the ServiceNow multi-provider SSO plugin.
### Properties

The SAML 2.0 Update 1 plugin includes the following system properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Identity Provider URL which will issue the SAML2</td>
<td>Enter the value of the <strong>Issuer</strong> element that the integration uses to validate the IdP URL. Each IdP URL must be unique.</td>
</tr>
<tr>
<td>security token with user info.</td>
<td>glide.authenticate.sso.saml2.idp</td>
</tr>
<tr>
<td>Sign LogoutRequest. Set this property to true if the Identity Provider's</td>
<td>Select whether the IdP requires a signed logout request.</td>
</tr>
<tr>
<td>SingleLogoutRequest service requires signed LogoutRequest.</td>
<td>glide.authenticate.sso.saml2.require_signed_logoutrequest</td>
</tr>
<tr>
<td>Select whether the IdP requires a signed logout request.</td>
<td>glide.authenticate.external.logout_redirect</td>
</tr>
<tr>
<td>The audience URI that accepts SAML2 token. (Normally, it is your instance</td>
<td>Enter the URL where the integration redirects users after they log out. Typically, you set this property to a UI page if you are using Kerberos authentication to prevent users from being redirected back to the IdP and logging in again after a logout request.</td>
</tr>
<tr>
<td>URL. For example: https://&lt;instance name&gt;.service-now.com.)</td>
<td>glide.authenticate.sso.saml2.audience</td>
</tr>
<tr>
<td>Create an AuthnContextClass request in the AuthnRequest statement.</td>
<td>Select whether to create an AuthnContextClass element in the SAMLRequest that specifies the login mechanism the IdP should use to authenticate the user. Not all IdPs support a AuthnContextClass element in the SAMLRequest. If you select <strong>Yes</strong>, you must specify the URN of the context class with the glide.authenticate.sso.saml2.authncontextclassref property.</td>
</tr>
<tr>
<td>glide.authenticate.sso.saml2.createrequestedauthncontext</td>
<td></td>
</tr>
<tr>
<td>The AuthnContextClassRef method that we will request in our SAML 2.0</td>
<td>Enter the URN of the login mechanism you want the IdP to use to authenticate users. For example, by default the system uses the forms-based Password Protected Transport authentication context urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport.</td>
</tr>
<tr>
<td>AutnRequest to the Identity Provider</td>
<td>glide.authenticate.sso.saml2.authncontextclassref</td>
</tr>
<tr>
<td>The alias of key entry stored in SAML 2.0 SP Keystore used to sign SAML 2</td>
<td>Enter the alias of the key that signs SAML 2 logout requests. You will have to create a Java Keystore for the alias.</td>
</tr>
<tr>
<td>requests.</td>
<td>glide.authenticate.sso.saml2.signing_key_alias</td>
</tr>
<tr>
<td>The password of key entry stored in SAML 2.0 SP Keystore used to sign SAML 2</td>
<td>Enter the password for the key that signs SAML 2 logout requests.</td>
</tr>
<tr>
<td>requests.</td>
<td>glide.authenticate.sso.saml2.signing_key_password</td>
</tr>
<tr>
<td>The number in seconds before “notBefore” constraint, or after “notOnOrAfter” constraint, to consider still valid.</td>
<td>Enter the number of seconds between the two attributes that make up the SAMLResponse nonce. A valid SAMLResponse must fall between the <strong>notBefore</strong> and <strong>notOnOrAfter</strong> date-time values.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>AuthnRequest URL for eSignature Authentication.</td>
<td>com.snc.integration.saml_esig.idp_authnrequest_url</td>
</tr>
<tr>
<td>The SAML 2.0 Assertion Consumer URL for eSignature authentication.</td>
<td>com.snc.integration.saml_esig.approval_consumer_url</td>
</tr>
<tr>
<td>The SAML 2.0 Assertion Consumer Index for eSignature authentication.</td>
<td>com.snc.integration.saml_esig.assertion_consumer_service_index</td>
</tr>
<tr>
<td>Authentication Pop-up Dialog Width.</td>
<td>com.snc.integration.saml_esig.popup_dlg_width</td>
</tr>
<tr>
<td>Authentication Pop-up Dialog Height.</td>
<td>com.snc.integration.saml_esig.popup_dlg_height</td>
</tr>
</tbody>
</table>

**SAML 2.0 update 1 requirements**

The SAML 2.0 update requires:

- Activating the SAML 2.0 Update 1 plugin
- Additional metadata from the SAML 2.0 Identity Provider (IdP)
  - SAML Request can include an `AuthnContextClass` element to specify the Service Provider's preferred login mechanism such as form-based authentication or Kerberos. If this element is not specified, the IdP chooses the login method.
  - SAML Response must include an `Issuer` element that matches the value listed in the issuer system property
  - SAML Response must include `SubjectConfirmation` and `SubjectConfirmationData` elements with a `Recipient` attribute
  - SAML Response must include `AudienceRestriction` and `Audience` elements that match the value listed in the audience system property

**SAML 2.0 integration requirements**

The SAML 2.0 integration requires several items, such as an IdP that provides a certificate and a single logout service.

- Activating the latest SAML 2.0 plugin
• Access to a SAML 2.0 Identity Provider (IdP)
  • Must provide an authentication request service
  • Must provide a single logout service
  • Must have a valid certificate
  • Must accept Service Provider (SP) metadata
  • Must use the NameID element in the SAMLResponse

Upgrade from previous versions

The following table lists the actions to take if you are running a previous versions of SAML.

<table>
<thead>
<tr>
<th>Previous SAML version</th>
<th>Action required</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML 1.1</td>
<td>Contact Customer Service and Support to migrate your instance to SAML 2.0 Update 1.</td>
</tr>
<tr>
<td>SAML 2.0</td>
<td>Update to SAML 2.0 Update 1.</td>
</tr>
</tbody>
</table>

Integrating SAML 2.0 with other features

You can integration your SAML 2.0 solution with other features like E-Signature, deep linking, and ADFS.

Add E-Signature support for SAML

Configure the following properties for E-Signature with SAML 2.0 update 1.

When E-signature is active with Multi-SSO, SAML properties are not used. The system adds E-signature properties to the SAML2 Update1 Properties [saml2_update1_properties] table:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assertion Consumer Index for eSignature authentication</td>
<td>An index number that identifies the endpoint.</td>
<td>1</td>
</tr>
<tr>
<td>Assertion Consumer URL for eSignature authentication</td>
<td>The URL that identifies the consumer.</td>
<td><a href="https://yourinstance.service-now.com/consumer.do">https://yourinstance.service-now.com/consumer.do</a></td>
</tr>
<tr>
<td>AuthnRequest URL for eSignature Authentication</td>
<td>The URL for authentication</td>
<td>none</td>
</tr>
</tbody>
</table>

If you are using E-Signature with SAML 1.0 or SAML 2.0 (not including update 1), see the special configuration instructions: Using E-Signature with Single Sign-On (SSO).

Note: If you are a Life Science Customer using E-Signature, deactivate the User self-lockout prevention business rule.

Add deep linking support for SAML

Deep linking allows instances to support direct email links to a particular record in the system.

With the SAML 2.0 integration enabled, deep-linking URLs must pass an authentication check before the IdP redirects the user to the originally requested URL. For example, consider an email that contains this URL: https://<instance name>.service-now.com/nav_to.do?url=incident.do?sys_id=46c88ac1a9fe1981014de1c831fbcf6d
The instance sends an authentication request to the IdP and uses the `RelayState` URL parameter to preserve the originally requested resource (in this case, `uri=incident.do?sys_id=46c88a1a9fe1981014d1c831fbc6d`). After the IdP authenticates the user, the instance reads the value of the `RelayState` URL parameter and redirects the user to the requested resource (if it exists in the instance).

To add support for deep linking verify that the identity provider supports the `RelayState` URL parameter.

**ADFS integration with SAML 2.0**

The ServiceNow Multi-Provider SSO plugin supports a SAML 2.0 single sign-on (SSO) integration with Microsoft Active Directory Federation Services (ADFS).

For information about installing and configuring ADFS, see Active Directory Federation Services Overview. The Multi-Provider SSO plugin has been configured and tested with a SAML 2.0 SSO integration with ADFS 2.0, 3.0, and 4.0. An integration with ADFS 5.0 might also be compatible.

**Note:** Multi-line attributes are not supported in the SAML Response in ServiceNow for ADFS.

**Set up ADFS for SAML**

This procedure uses ADFS 2.0 and shows samportal.example.com as the ADFS website. Replace this with your ADFS website address.

Role required: admin

1. Log into the ADFS 3.0 server and open the management console.
2. Right-click **Service** and choose **Edit Federation Service Properties**.
3. Confirm that the General settings match your DNS entries and certificate names.

4. Browse to the certificates and export the Token-Signing certificate.
   a) Right-click the certificate and select **View Certificate**.
   b) Select the **Details** tab.
   c) Click **Copy to File**. The Certificate Export Wizard opens.
   d) Select **Next**.
   e) Ensure the **No, do not export the private key** option is selected, and then click **Next**.
   f) Select **DER encoded binary X.509 (.cer)**, and then click **Next**.
   g) Select where you want to save the file and give it a name. Click **Next**.
   h) Select **Finish**. The instance requires that this certificate be in PEM format. You can convert this certificate using client tools or even online tools such as: SSL Shopper.
5. Use the DER/Binary certificate that you just created, and export it in Standard PEM format.

Set up the instance for ADFS
Once you have set up ADFS for SAML, you can configure your instance and SAML 2.0 settings to work with ADFS.
Role required: admin

1. If not already active, activate the Integration - Multiple Provider Single Sign-On Installer plugin.
2. Configure Authentication with SAML, but when you install the IdP certificate, attach the PEM certificate you created when you Set up ADFS for SAML.
3. Click Save.
4. Verify that the Issuer and Subject fields have values and that there are no errors. If an error occurs, open the saved PEM formatted certificate in Notepad and copy and paste the certificate into the PEM Certificate field.
5. Verify that the SAML2SingleSignon_update1 installation exit is active.
6. Continue the SAML 2.0 configuration.

**Note:** When a certificate is updated on the ADFS server, you also need to upload an updated certificate to the instance.

Configure an ADFS relying party
At this point you can take the instance metadata and import it into your ADFS server. However, manual configuration of the relying party appears to be easier to implement.
Role required: admin

1. Navigate to Multi-Provider SSO > Identity Providers > SAML2 Update1 > Encryption And Signing and verify that the SAML property Sign AuthnRequest (glide.authenticate.sso.saml2.require_signed_authnrequest) is not active. Only keep this property active if your ADFS administrator can verify that you require signed requests.
2. Copy the metadata that you generated through the SAML 2 metadata link and save it to a file.
3. Log into the ADFS server and open the management console.
5. Select Add Relying Party Trust from the top right corner of the window.
   The add wizard appears.
6. Click Start to begin.
7. Use the Import File option to import the metadata file.
8. Give it a display name such as ServiceNow and enter any notes you want.
9. Select ADFS 3.0 Profile.
10. Do not select a token encryption certificate. It will use the certificate that is defined on the service that has already been exported. Defining a certificate here will prevent proper communication with the instance.
11. Do not enable any settings on the Configure URL.
12. Enter the instance site to which you connected as the Relying Party trust identifier. In this case use https://company.service-now.com and click Add.
13. Permit all users to access this relying party.
14. Click Next and clear the Open the Claims when this finishes check box.
15. Close this page. The new relying party trust appears in the window.
16. Right-click on the relying party trust and select Properties.
17. Browse to the Advanced tab and set the Secure hash algorithm. You can choose SHA-256 or SHA-1.

Configure ADFS relying party claim rules
Edit the Claim rules to enable proper communication with the instance.

Role required: admin

1. Log into the ADFS server and open the management console.
2. Right-click the relying party trust and select **Edit Claim Rules**.
3. Click the **Issuance Transform Rules** tab.
4. Select **Add Rules**.
5. Select **Send LDAP Attribute as Claims** as the claim rule template to use.
6. Give the claim a name such as **Get LDAP Attributes**.
7. Set the **Attribute store** to Active Directory, the **LDAP Attribute** to E-Mail-Addresses, and the **Outgoing Claim Type** to E-mail Address.

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"]
```
8. Select Finish.
9. Select Add Rules.
10. Select Transform an Incoming Claim as the claim rule template to use.
11. Give the Claim a name such as Email to Name ID.
12. Set the Incoming claim type to the Outgoing Claim Type in the previous rule. For example, E-Mail Address.
13. Set the Outgoing claim type to Name ID and the Outgoing name ID format to Email.

Note: These values must match the Name ID policy you define during SAML 2.0 configuration.
14. Select **Pass through all claim values**.

This claim rule should look similar to the following rule language.

```c
[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
```
Create a SAML logout endpoint
Create a SAML logout endpoint to allow single logout.
Role required: admin
See this article on ADFS signout for more information.

Note: An IdP initiated logout is not supported.

1. Go to ADFS manager > Trust Relationships > Relying Party Trusts > properties.
2. Under the Endpoints tab, click Add SAML.
3. Configure the settings:
   - Endpoint Type: SAML Logout
   - Binding: POST
   - Trusted URL: The URL of your ADFS server. For example,
     https://myadfsserver.domain.net/adfs/ls/?wa=wsignout1.0
   - Response URL: The application logout URL. For example,
     https://{instancename}.service-now.com/external_logout_complete.do

Test the ADFS configuration
Test your ADFS configuration to verify that it is properly functioning as an identity provider.
Role required: admin
1. Open an Internet Explorer browser.
   This page contains a drop down list of all configured Relying Party Trusts.
3. Select the relying party associated with your instance.
4. Click Continue to Sign In.
   If you have configured the SAML 2.0 external authentication properly, you should be automatically logged into the instance.

(Workaround) Enable service provider-initiated authentication
A workaround is available if authentication fails because you do not have SAML 2.0 Update 1. This can happen if users attempt to skip IdP authentication and navigate directly to the instance.
Role required: admin
This is an error with the instance not providing ADFS with the needed definition and semantics for the SPNameQualifier attribute in the SAMLResponse.
To enable service provider-initiated authentication, do one of the following

- Upgrade to SAML 2.0 Update 1 and clear the option to create an AuthnContextClass request. See Activate and set up SAML 2.0.
- Modify the SAML2 script include to comment out the definitions of the SPNameQualifier attribute when you have SAML 2.0 active (not SAML 2.0 Update 1).

Comment out these lines in the createNameID and createNameIDPolicy functions:

```java
//nid.setSPNameQualifier (serviceURL ) ;
//nameIdPolicy. setSPNameQualifier (serviceURLStr ) ;
```

If you do not want the login prompt from your ADFS server to appear when you access the instance, set the following SAML 2.0 Update 1 property to false: Create an AuthnContextClass request in the AuthnRequest statement (`glide.authenticate.sso.saml2.createrequestedauthncontext`).

(Workaround) Support Kerberos authentication

A workaround is available for the SAML 2.0 integration that changes the authentication context from forms-based authentication to Windows-based authentication.

Role required: admin

Currently, the SAML 2 integration uses a PasswordProtectedTransport or "forms-based authentication" authentication context. This authentication context requires the IdP to present users with a form for authentication credentials. With Kerberos, a SAML session is already active through an established Windows login, so the user does not need to authenticate with the IdP.

1. Navigate to Multi-Provider SSO > Identity Providers.
2. Open the SAML2 Update1 IdP record.
3. Set the The AuthnContextClassRef method that we will be included in our SAML 2.0 AuthnRequest to the Identity Provider to one of the following:

```
AuthnContextClassRef method values

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</td>
<td>(Default)</td>
</tr>
<tr>
<td>urn:federation:authentication:windows</td>
<td></td>
</tr>
</tbody>
</table>
```

4. Click Update.

Email links with external authentication

You can use email links when using the digestive token external authentication, however, you must establish how to handle links in email notifications.

The default links contain a URL that directs you to a specific location in the instance, like an Incident or Change Request, without incorporating SSO credentials. Below are examples for directing the user to the location in the instance without logging in on the instance login page.

- Unencrypted HTTP technique to connect to the /demo instance (it does not navigate to specific record):

  ```
  https://<instance name>.service-now.com/?
  SM_USER=user_name&DE_USER=1QjIVp7aRJtyPx5+2O/vgU24tbE=
  ```

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
• Link (in an email notification) to a specific record, so that the user first goes to the company's own login portal:

```
https://login.company_portal_page.com/nav_to.do?uri=incident.do?
sys_id=009f8eda0a0b2b01ab4eb094223466%26sysparm_stack=incident_list.do
%3Psparm_query=active=true
```

You must set the `glide.email.override.url` property in your instance to contain the URL of the company portal page. If this property does not exist, you can create it.

• The company portal must then take that URL and construct the redirect URL to the instance preserving the segment necessary to access the specific record, and adding the SSO credentials to the end of the URL:

```
https://<instance name>.service-now.com/nav_to.do?uri=incident.do?
sys_id=009f8eda0a0b2b01ab4eb094223466%26sysparm_stack=incident_list.do
%3Psparm_query=active=true&SM_USER=user_name&DE_USER=1QjIVp7aRJtyPx5+2O/ 
vGU24tbE=
```

Migrating an existing SAML 1.1 integration to SAML 2.0

To migrate from a SAML 1.1 integration to a SAML 2.0 integration, contact customer support.

Update existing SAML 2.0 integration

Perform these steps to update your existing SAML 2.0 integration.

Role required: admin

Request the SAML 2.0 Update 1 Plugin

Contact Customer Service and Support to request the `SAML 2.0 Single Sign-On - Update 1: security enhancements` plugin. The plugin applies updated versions of the `SAML2SingleSignon` installation exit (login script), `SAML2Logout` installation exit (logout script), and `SAML2` script include (script object).

Merge Customizations from Existing Installation Exit Scripts into New Scripts

The update saves an inactive copy of the integration's original installation exit scripts. You can use these copies to merge any customizations you made to the login and logout scripts to the new versions of these installation exits.

```
<table>
<thead>
<tr>
<th>Original Installation Exit Script Name</th>
<th>Original Script Status</th>
<th>New Installation Exit Script Name</th>
<th>New Script Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML2SingleSignon</td>
<td>Inactive</td>
<td>SAML2SingleSignon_update</td>
<td>Active</td>
</tr>
<tr>
<td>SAML2</td>
<td>Inactive</td>
<td>SAML2_update1</td>
<td>Active</td>
</tr>
<tr>
<td>SAML2Logout</td>
<td>Inactive</td>
<td>SAML2Logout_update1</td>
<td>Active</td>
</tr>
</tbody>
</table>
```

You can navigate to the SAML 2.0 login and logout installation exit scripts using these paths.

• **SAML 2 Single Sign-on > Login script.**
• **SAML 2 Single Sign-on > Logout script.**
• **System Definition > Installation Exits.**

You can navigate to the SAML 2.0 update 1 script include using these paths.

• **SAML 2 Single Sign-on > Script object.**
• **System Definition > Script Includes.**

Test the Update
Perform these steps to troubleshoot your integration update.

1. Add a system property called `glide.authenticate.sso.saml2.debug` with a value of `true`.
2. Attempt SAML 2.0 login.
3. Review the system log. SAML2 validation errors begin with the text `SAML2ValidationError`.
4. Identify and fix typical login errors. See Multi-SSO (SAML 2.0) errors and fixes.

Sample SAML 2 responses after the update

The following sections illustrate the new required elements and attributes that the IdP should provide in the SAML Response.

Sample SAML 2 Response with Issuer Element

The following SAML 2 response uses the `Issuer` element.

```xml
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    Destination="https://demoi2.service-now.com/navpage.do"
    ID="s28da6774c88ae1eab292bf25fe625db81919d8e"e"
    InResponseTo="SNC841720c227c81948cf6d68cad6235c6"
    IssueInstant="2012-01-30T20:07:10Z"
    Version="2.0">
    <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
        http://idp.ssocircle.com
    </saml:Issuer>
    ...
    <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
        ID="s2f347f973c0633836cf700a38302d94976f9c5b851"
        IssueInstant="2012-01-30T20:07:10Z"
        Version="2.0">
        http://idp.ssocircle.com</saml:Issuer>
    ...
</saml:Assertion>
</samlp:Response>
```

Sample SAML 2 Response with the SubjectConfirmation and SubjectConfirmationData Elements

The following SAML 2 response uses the `SubjectConfirmation` and `SubjectConfirmationData` elements with the `NotOnOrAfter` and `Recipient` attributes.

```xml
<saml:SubjectConfirmationMethod="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <saml:SubjectConfirmation
        InResponseTo="SNC841720c227c81948cf6d68cad6235c6"
        NotOnOrAfter="2012-01-30T20:17:10Z"
        Recipient="https://demoi2.service-now.com/navpage.do"/>
</saml:SubjectConfirmation>
```

Sample SAML 2 Response with the AudienceRestrictions and Audience Elements

The following SAML 2 response uses the `AudienceRestrictions` and `Audience` elements with the `NotBefore` and `NotOnOrAfter` attributes.

```xml
<saml:ConditionsNotBefore="2012-01-30T19:57:10Z"
    NotOnOrAfter="2012-01-30T20:17:10Z">
    <saml:AudienceRestriction>
        https://demoi2.service-now.com/navpage.do</saml:AudienceRestriction>
</saml:Conditions>
```
SAML user provisioning

If users exist in your IdP but are not in your instance, SAML user provisioning can automatically create the users in your instance’s User [sys_user] table.

SAML user provisioning is supported for SAML 2.0 Update 1 when Multi-SSO is enabled.

How SAML user provisioning works

When SAML user provisioning is enabled and the system encounters a new user that is not in the instance, the instance automatically creates a record in a temporary table with the name u_imp_saml_user_<suffix>, where <suffix> is an automatically generated text identifier. The system also creates transform map that specifies the data relationships between the import table and the User table. Each IdP in identified in the system has its own transform map. The transform map is created once for each IdP. Administrators can update it as necessary.

When the user logs in, they access an IdP to log in.

- The system presents a list of all IdPs that are able to use SAML user provisioning. If there is only one IdP that can use SAML user provisioning, that one is used automatically.
- If none of the above conditions are true, the system uses the Auto Redirect IdP.

Administer SAML user provisioning

To update the User table with the users in your IdP, you must first set up field mapping and then enable user provisioning through Multi-SSO IdP settings.

Set up your IdP mapping to identify what fields in the IdP are mapped to the correct fields in the User table.

Role required: admin

1. Navigate to Multi-Provider SSO > Properties.
2. Select Enable Auto Importing of users from all identity providers into the user table (glide.authenticate.multisso.user.autoprovision) to activate this feature.
3. Click Save.
5. Open the SAML2 Update1 record.
6. To create a record in the User table when the user does not already exist, select Auto-provision Users. If you upgraded to this release, you need to configure the form and add this field.
7. To enable user records to be updated when users log in to the IdP and the information on the IdP is out of date with the information on the User table, select Update User Record Upon Each Login. If you upgraded to this release, you need to configure the form and add this field.
8. Click User Provisioning Transform Map to see the map that the system automatically creates.
9. Make changes to the map as needed.

When the first unknown user tries to log in, the system creates the fields in the import set table from the metadata.xml file.

Note: You cannot map the fields from the IdP table until this first user logs in.

SAML 2.0 troubleshooting

Before contacting support, try the troubleshooting solutions available in the knowledge base on Hi.

Note: The instance does not support solutions provided by external sites.

See the following knowledge base article: KB0540617 "SAML Error Matrix".
### Other Common Issues

<table>
<thead>
<tr>
<th>Error or Symptom</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error message: &quot;is not a function.&quot;</td>
<td>This error occurs because the plugin was not active and did not load the .jar file. Therefore, the code appears to be missing. Contact Technical Support to restart nodes that are missing the plugin.</td>
</tr>
<tr>
<td>SAML does not authenticate users accessing CMS pages.</td>
<td>By default, CMS pages are public and therefore do not require authentication. If you want SAML to authenticate CMS pages, change the <code>view_content.do</code> public page from <code>active=true</code> to <code>active=false</code>.</td>
</tr>
<tr>
<td>Cannot redirect a user back to a CMS page after SAML authentication.</td>
<td>By default, the SSO integration uses a URL parameter called <code>URI</code> to control where the user is directed after authentication at the IdP. SSO ignores relative URLs. For example, SSO cannot redirect users to a <code>/ess</code> relative URL. Instead, the user has to navigate to a URL such as <code>/nav_to.do?uri=/ess</code>, which uses deep linking syntax. However, this puts the ESS portal inside the main navigation content IFrame. In other words, the site does not take up the full page, but rather loads as a page in your instance. For more information, see CMS Sites and Single Sign-On. If you change the CMS entry page to make it private by setting <code>view_content.do</code> to <code>active=false</code>, deep linking behavior then requires a customization to the Installation Exit login script. Create a script that looks for the <code>URI</code> portion of the URL and constructs a <code>RelayState</code> URL parameter containing the relative URL path to redirect users after authenticating at the IdP.</td>
</tr>
<tr>
<td>SAML does not redirect users to the appropriate page after authentication.</td>
<td>Determine if the relay state is passed out to the IdP and then passed back during authentication. You can do this with a browser capable of saving HTTP request headers and POST info, such as Chrome with its built-in developer tools, or Firefox with the add-on called HTTPfox. For Internet Explorer, use a third-party application such as Fiddler. The goal is to watch the requests pass from the client (browser) to the instance, and from the client to the IdP.</td>
</tr>
</tbody>
</table>

**Monitor the event queue for login activities**

Every single sign-on integration creates events for login activities.

You can use these events to monitor for login failures and determine if there are any security concerns to address.

**Monitoring the event queue for login failures**

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Description</th>
<th>Record</th>
<th>Parameter 1</th>
<th>Parameter 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>external.authentication.succeeded</code></td>
<td>authentication succeeded and the user accessed the instance URL.</td>
<td>Session ID</td>
<td>User ID of user who successfully logged in</td>
<td>The URL the user accessed (which may be a deep link)</td>
</tr>
<tr>
<td>Event Name</td>
<td>Description</td>
<td>Record</td>
<td>Parameter 1</td>
<td>Parameter 2</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------------</td>
<td>-------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td><code>external.authentication.failed</code></td>
<td>The single sign-on requirements are not present or are missing.</td>
<td>Session ID</td>
<td>Session ID</td>
<td>The missing authentication requirements</td>
</tr>
<tr>
<td><code>external.authentication.failed</code></td>
<td>The user does not exist in the User [sys_user] table.</td>
<td>User ID</td>
<td>User ID</td>
<td>The string, &quot;User does not exist&quot;</td>
</tr>
<tr>
<td><code>external.authentication.failed</code></td>
<td>The user is locked out.</td>
<td>User ID</td>
<td>User ID</td>
<td>The string, &quot;User locked out.&quot;</td>
</tr>
</tbody>
</table>

**Event queue login events**

The SAML 2.0 integration creates events for login activities.

You can use these events to monitor for login failures and determine if there are any security concerns to address.

**Login activities events**

<table>
<thead>
<tr>
<th>Event name</th>
<th>Description</th>
<th>ID used with event</th>
<th>Event string</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>saml2.logout.validation.failed</code></td>
<td>The logout response from the IdP failed validation against your logout request. The event validates the &lt;inResponseTo&gt; element against the session ID (ID attribute of the <a href="">saml2p:LogoutRequest</a> element). For example, see the workflow for logout request issued.</td>
<td>Session ID</td>
<td>The string, &quot;SAML2 LogoutResponse validation failed.&quot;</td>
</tr>
<tr>
<td><code>external.authentication.succeeded</code></td>
<td><code>External authentication failed.</code></td>
<td>The string, 'Authentication failed'</td>
<td></td>
</tr>
<tr>
<td><code>external.authentication.succeeded</code></td>
<td><code>External authentication succeeded and the user accessed the instance URL.</code></td>
<td>Session ID &amp; User ID of user who successfully logged in</td>
<td>The URL the user accessed (which may be a deep link)</td>
</tr>
<tr>
<td><code>external.authentication.failed</code></td>
<td>The single sign-on requirements are not present or are missing.</td>
<td>Session ID</td>
<td>The missing authentication requirements</td>
</tr>
<tr>
<td><code>external.authentication.failed</code></td>
<td>The user does not exist in the User [sys_user] table.</td>
<td>User ID</td>
<td>The string, 'User does not exist'</td>
</tr>
<tr>
<td><code>external.authentication.failed</code></td>
<td>The user is locked out.</td>
<td>User ID</td>
<td>The string, 'User locked out'</td>
</tr>
</tbody>
</table>

**Certificate-based authentication**

Certificate-based authentication lets you mutually authenticate user logins or inbound API requests using certificates from a trusted Certificate Authority (CA).

**Certificate-based authentication for user interface logins**
Enable end users to use PIV (Personal Identity Verification) or CAC (Common Access Card) cards to log in to the Now Platform or Service Portal instead of using a user name and password. To set up mutual authentication for user interface logins, see Set up Certificate-based authentication.

After Certificate-based authentication is set up, end users can finalize their setup and log in. See Log in using Certificate-based authentication.

Certificate-based authentication for Inbound web services

Authenticate inbound requests to ServiceNow SOAP and REST APIs. To set up mutual authentication for inbound web services, see Set up Certificate-based authentication.

Set up Certificate-based authentication

Set up mutual authentication for either user interface-based logins or inbound web services.

Role required: admin

Check that your instance is using an ADCv2 load balancer. For more information, see the ADCv2 Migration knowledge article. If your instance is not using the ADCv2 load balancer, contact Now Support.

Set up Certificate-based authentication in order to:

• Allow end users to securely log in to the Now Platform or Service Portal using PIV or CAC cards. After certificate-based authentication is enabled, you can self-register the PEM certificate or an administrator can map the certificate for you. See Log in using Certificate-based authentication.

• Enable mutual authentication for inbound web services. Once certificate-based authentication is set up, the system uses the provided certificates to mutually authenticate requests to access ServiceNow REST and SOAP APIs.

Activate Certificate-based authentication

You can activate the Certificate based authentication plugin (com.glide.auth.mutual) for Now Platform if you have the admin role.

Role required: admin

The following items are installed with Certificate based authentication:

• Scheduled jobs: Poll LB For Certificate Status
• Tables: sys_user_certificate, sys_ca_certificate, sys_ca_certificate_api_track

1. Navigate to System Applications > All Available Applications > All.
2. Find the Certificate based authentication plugin (com.glide.auth.mutual) using the filter criteria and search bar.
   You can search for the plugin by its name or ID. If you cannot find a plugin, you might have to request it from ServiceNow personnel. For more information, see Request a plugin.
3. Click Install, and then in the Activate Plugin dialog box, click Activate.

   Note: When domain separation and delegated admin are enabled in an instance, the administrative user must be in the global domain. Otherwise, the following error appears:
   Application installation is unavailable because another operation is running: Plugin Activation for <plugin name>.

Register CA certificate

Register root certificates or intermediate certificates to make them available for authentication.

Role required: admin

1. Navigate to Certificate Based Authentication > CA Certificate Chain.
2. Click New.
3. On the form, fill in the fields:

**Mutual Auth CA Certificate form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name to identify the certificate.</td>
</tr>
<tr>
<td>Expiration notification</td>
<td>Option to warn users when a certificate is about to expire.</td>
</tr>
<tr>
<td>Notify on expiration</td>
<td>List of users to be notified when the certificate expires.</td>
</tr>
<tr>
<td>Warn in days to expire</td>
<td>Number of days when a notification is sent to users before a certificate expires.</td>
</tr>
<tr>
<td>Active</td>
<td>Option to make the client certificate active.</td>
</tr>
<tr>
<td>Format</td>
<td>PEM</td>
</tr>
<tr>
<td>Type</td>
<td>Type of certificate. Options include:</td>
</tr>
<tr>
<td></td>
<td>• CA Cert: The root CA certificate. Can also include intermediate certificates in the chain. CA certificates are automatically sync with the load balancer. Use this option when possible to avoid missing a required certificate in the chain.</td>
</tr>
<tr>
<td></td>
<td>• Intermediate Cert: An intermediate certificate in the certificate chain. This certificate remains on the instance only and is not sync with the load balancer. Only use this option if you need to add an intermediate certificate to an existing chain.</td>
</tr>
<tr>
<td>Short description</td>
<td>Short description of the user client certificate.</td>
</tr>
</tbody>
</table>

**Note:** During the certificate upload, the read-only fields, **Valid from, Expires, Expires in days, Issuer, and Subject, Certificate Chain, and PEM Certificate** are extracted and auto-populated.

4. Click **Submit**.

5. Optional: Click Validate Stores/Certificates to validate the certificate.

**Map PEM certificate to user**

Map PEM certificates to users to enable them to log in using PIV or CAC cards or to authenticate inbound requests. You can map multiple PEM certificates to a user.

- Role required: admin
- Make sure that you have the Privacy Enhanced Mail (PEM) certificate of the user.

1. Navigate to **Certificate Based Authentication > User to Certificate Mapping**, and click **New**.
2. On the form, fill in these fields:

**User Client Certificate form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the user client certificate.</td>
</tr>
<tr>
<td>Expiration notification</td>
<td>Option to warn users when a certificate is about to expire.</td>
</tr>
<tr>
<td>Warn in days to expire</td>
<td>Number of days when a notification is sent to users before a certificate expires.</td>
</tr>
<tr>
<td>Notify on expiration</td>
<td>List of users to be notified when the certificate expires.</td>
</tr>
<tr>
<td>Active</td>
<td>Option to make the client certificate active.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>User who is mapped to the client certificate. The system receives the client certificate from either the inbound request or certificate registration, and then uses the user designated in this field to initiate a session to execute the request.</td>
</tr>
<tr>
<td>Short description</td>
<td>Short description of the user client certificate.</td>
</tr>
<tr>
<td>Format</td>
<td>PEM. Privacy Enhanced Mail (PEM) format is a base-64 encoded Distinguished Encoding Rules (DER) certificate.</td>
</tr>
<tr>
<td>Type</td>
<td>Client cert. This field is read only.</td>
</tr>
</tbody>
</table>

**Note:** During the certificate upload, the read-only fields, **Valid from**, **Expires**, **Expires in days**, **Issuer**, and **Subject** are extracted and auto-populated.

3. Click the attachments icon and upload the certificate.
4. Click **Submit**. The certificate is validated and mapped to the specified user if the certificate is from a trusted Certificate Authority (CA).

Configure Certificate-based authentication properties
Configure Certificate-based authentication properties.

Role required: **admin**

1. Navigate to **Certificate Based Authentication > Properties**.
2. On the form, fill in the fields:

#### Certificate Based Authentication Properties form

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable certificate based authentication</td>
<td>Option to enable to certificate-based authentication for both user interface logins and inbound web services. Default: true</td>
</tr>
<tr>
<td>Show 'Log in with PIV/CAC' option in login screen</td>
<td>Displays the <strong>Log in with PIV/CAC card</strong> option on the login screen. Allows users to log in using certificate-based authentication using the user interface. Default: false</td>
</tr>
</tbody>
</table>

**Log in using Certificate-based authentication**

After your administrator sets up Certificate-based authentication, you can register the client certificate and log in using your PIV (Personal Identity Verification) or CAC (Common Access Card) card.

**Register client certificate for your PIV or CAC card**

Before you log in to Now Platform using your PIV or CAC card, you must register the client certificate of your PIV or CAC card. If you are not able to register the client certificate, contact your administrator. Your administrator can also register the client certificate of your PIV or CAC card.

- Make sure that certificate-based authentication is enabled.
- Make sure that a card reader is connected to your computer and your PIV or CAC card is inserted.
• Role required: none

1. Log in to Now Platform using your user name and password.
2. Click your name from the User Menu and select Profile.
3. From the Related Links, click Register client certificate. If a valid is certificate is available, the following message displays:

![PIV/CAC Certificate Found dialog box]

Register your PIV/CAC certificate to use it for future login

Certificate

PIVKey

[Cancel] [Register]
4. Click **Register**.

After the registration is successful, the following message displays:

The PIV/CAC certificate has been successfully registered and linked to the user account.

**Note:** If a certificate is already registered to you or other users, you cannot register the same certificate again to yourself.
The next time you log in to your Now Platform, you can log in using your PIV or CAC card. For more information, see Log in to Now Platform using PIV or CAC card.
Log in to Now Platform using PIV or CAC card

You can log in with your PIV or CAC card instead of user name and password when certificate-based authentication is enabled on Now Platform.

- Role required: none
- Make sure that certificate-based authentication is enabled.
- Make sure that a PIV or CAC card reader is connected to your computer.
- Make sure that a client certificate of your PIV or CAC card is mapped to you. For more information, see Register CA certificate.

1. Insert your PIV or CAC card into the card reader.
2. Navigate to your instance in a browser.
   Browser prompts for a PIN for your PIV or CAC card.
3. Enter the PIN of your PIV or CAC card in the browser prompt.
   
   **Note:** If you forget your PIN, contact your administrator.

4. If you enter a correct PIN, the browser displays a prompt to select a certificate.
5. Select a certificate from the browser prompt.
   If the certificate is valid and mapped to you, you are redirected to the login page.

6. Click **Log in with PIV/CAC card** button.
   To log out of the Now Platform, you must remove the PIV or CAC from the card reader and then close the browser.

**Limit concurrent sessions**

You can limit the number of concurrent interactive sessions for a user or role on an instance across all nodes.

Concurrent interactive sessions refer to the number of sessions a user can have active per ServiceNow instance. An active instance session occurs with every new login to a specific ServiceNow instance. By default, there are no limitations on the number of active instance sessions a user can have.

With the Jakarta release, you can limit the number of active concurrent sessions per user. When the user logs in after hitting the maximum number of sessions active, the oldest active session terminates and a new interactive session becomes active. If a user tries to access a closed session through a browser, the user is redirected to the login page.

**Note:** The **Limit concurrent sessions** plugin must be active to enable a maximum session limit. Limits are set through the glide.authenticate.max.concurrent.interactive.sessions property. A maximum limit value applies to any user or role that has the limit property active. A user or a role connected to the user must have...
A typical use case if a maximum concurrent session of 1 is set:

1. The user accesses the initial ServiceNow instance through Chrome.
2. After the user successfully logs in, ServiceNow creates session 1 (S1) for the user.
3. The user decides to initiate another access to the ServiceNow instance through Firefox.
4. After the user successfully logs in, ServiceNow creates session 2 (S2) for the user.
5. Since the user has a maximum concurrent session limit of 1, the S1 session invalidates when S2 is created.
6. When the user goes back through Chrome to access the S1 ServiceNow instance, the user is redirected to the login page as S1 is invalid.

Concurrent session limits work with all the ServiceNow authentication mechanisms: SAML, LDAP, and local database authentication. It also works with Multi-factor authentication and all interactive ServiceNow authentication mechanisms. The source of the session is viewable through the `sys_user_session` table, under the column `Type`. The values can be:

- Web Browser
- Mobile Browser
- ServiceNow Mobile App
- Non-interactive (SOAP, WSDL, OAuth)

**Activate and configure limit concurrent sessions plugin**

You can activate the Limit Concurrent Sessions plugin (com.glide.limit.concurrent.sessions) if you have the admin role.

Role required: admin

1. Navigate to **System Definition > Plugins**.
2. Find and click the Limit Concurrent Sessions plugin.
3. On the System Plugin form, review the plugin details and then click the **Activate/Upgrade** related link.
4. Click **Activate**.
5. To enable this feature and set a maximum limit of concurrent sessions, go to the Plugin Files tab, find the following properties, and change the setting values:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>glide.authenticate.limit.concurrent.interactive.sessions</code></td>
<td>You can enable the ability to limit concurrent sessions by setting the value to <strong>True</strong>. By default, this property is set to <strong>False</strong>, which means there is no limit on the number of interactive sessions a user can have active.</td>
</tr>
<tr>
<td><code>Note:</code></td>
<td><strong>To disable this feature, set this property back to False.</strong></td>
</tr>
<tr>
<td><code>glide.authenticate.max.concurrent.interactive.sessions</code></td>
<td>You can set the maximum number of concurrent active interactive sessions a user can have on the instance across all nodes.</td>
</tr>
</tbody>
</table>
6. Optional: You can also amend the following properties, if necessary:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| glide.authenticate.session.types.to.limit.concurrency | This property limits session types. By default, only the web browser sessions have a limit. Session types include:  
    • Web Browser (1)  
    • Mobile Browser (2)  
    • ServiceNow Mobile App (3)  
    • Non-interactive (10)  

You can configure and set the value to '1' for web browser, '2' for mobile browser, or '1,2' for both.

| glide.authenticate.limit.concurrent.sessions.across.all.nodes | This property restricts the limit of concurrent sessions per node instead of restricting them across all nodes of a ServiceNow instance. By default, the value is set to true, which limits user sessions across all nodes. If the property is set to false, only the sessions on that node and not the ones on the other nodes are subject to the limit. |

7. Click Update to have the settings take effect.

Set a concurrent session limit by user or role

You can set a concurrent session limit on a specific user or on a particular role.

Role required: admin

1. Navigate to User Administration > Users or User Administration > Roles.
2. Select a user or role that you want to set a concurrent session limit, check the Limit Concurrent Sessions check box, and click Update.
   The user or role has a limit of how many concurrent sessions can be open at one time.

Disable a concurrent session limit by user or role

You can disable a concurrent session limit on a specific user or on a particular role.

Role required: admin

1. Navigate to User Administration > Users or User Administration > Roles.
2. Select a user or role that you want to disable a concurrent session limit, uncheck the Limit Concurrent Sessions check box, and click Update.
   The user or role is not subject to a limit of how many concurrent sessions can be open at one time.
OAuth 2.0

OAuth 2.0 lets users access instance resources through external clients by obtaining a token rather than by entering login credentials with each resource request.

You must have the security_admin role to manage the OAuth integration. Configure OAuth 2.0 for the following scenarios:

- **OAuth external client scenario**: Your instance provides an endpoint for third-party clients to pull data from the instance.
- **OAuth provider scenario**: Your instance pulls data from a third-party provider.

Both the simple security and high security frameworks support OAuth 2.0. High Security is recommended. See for information about which versions have high security already active and how to activate high security.

### Key concepts of the OAuth 2.0 implementation

<table>
<thead>
<tr>
<th>Concept</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Owner</td>
<td>An entity capable of granting access to a protected resource. A resource owner who is a person is called an <em>end user</em>. The resource owner is always a user account.</td>
</tr>
<tr>
<td>Client</td>
<td>An application that, with the authorization of the resource owner, makes requests for protected resources on behalf of the resource owner.</td>
</tr>
<tr>
<td>Resource Server</td>
<td>The server that hosts the protected resources, capable of accepting and responding to requests for protected resources.</td>
</tr>
<tr>
<td>Authorization Server</td>
<td>The server that issues access tokens to the client after successfully authenticating the resource owner and obtaining authorization.</td>
</tr>
<tr>
<td>Authorization Request</td>
<td>The permission that a client requires to access a protected resource. The authorization request is always an HTTP POST message that contains the ID of the client that is acting on behalf of the resource owner and credentials that authorize the request.</td>
</tr>
<tr>
<td>Authorization Grant</td>
<td>A credential that represents the authorization from the resource owner to access a resource. The authorization grant is either user login credentials or a refresh token.</td>
</tr>
<tr>
<td>Access Token</td>
<td>A secure string that a client uses to access protected resources. An instance issues access tokens to clients that have a valid authorization grant. Each access token has a specific scope, lifespan, and other attributes. By default, an instance issues access tokens with a 30-minute lifespan in the scenario where the instance is the OAuth provider. For third-party tokens, 30 days.</td>
</tr>
</tbody>
</table>
### ServiceNow DocVersion Now Platform administration

<table>
<thead>
<tr>
<th>Concept</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh Token</td>
<td>A credential that a client uses to obtain new access tokens without requiring additional user authorization. An instance issues a refresh token to a client when it is first authorized to have an access token. By default, an instance issues refresh tokens with a 100-day lifespan in the scenario where the instance is the OAuth provider. For third-party tokens, 365 days.</td>
</tr>
<tr>
<td>Self-signed certificates</td>
<td>The Now Platform does not support self-signed certificates. The OAuth client does not utilize the certificate trust store or allow connection to OAuth endpoints that incorporate a self-signed certificate.</td>
</tr>
<tr>
<td>User agent</td>
<td>The user who delegates access rights to a client application, which is often a website. The access rights permit the client application or website to access data in the instance that the user has access rights to. The user agent is used in the scenario.</td>
</tr>
</tbody>
</table>

### OAuth grant types

A **grant type** is the way that the client obtains the access token. The following grant types are supported:

- **Authorization code:** The consumer first gets an authorization code and then uses it to get an access token. You can Specify an OAuth profile and specify this grant type. The process that uses the authorization code is also referred to as **auth code flow** or **authorization code flow**.

- **Resource owner password credentials:** The consumer of the resource already has the user credentials to get the access token. This process is also referred to as **password flow**.

- **Client credentials:** The consumer of the resource uses the client ID and client secret that is already configured in the application registry.

### Storage of authentication credentials

The OAuth client secret is stored as a **password2** type field, which is encrypted in Triple DES. User passwords, which are used to check incoming endpoint requests, are stored as a hash value in the User table in a **password** type field (SHA 256).

### Set up OAuth

Set up and activate OAuth, enable the OAuth system property, create an OAuth application endpoint for external client applications to access the instance, and set OAuth parameters.

Role required: admin

1. Make sure the **OAuth plugin** is active and the **OAuth activation property** is set to true.
2. Create an OAuth application registry using one of the following methods:
   • Create an endpoint for external clients that want to access your instance. This creates an OAuth client application record and generates a client ID and client secret that the client needs to access the restricted resources on the instance.
   • Use a third-party OAuth provider that provides the authorization for access to your instance.
     Specify an OAuth profile and Specify an OAuth scope when you are connecting to another OAuth provider.

3. Configure your client applications to create an HTTP POST that requests an OAuth token. The application must also be able to parse the JSON response to use the returned access token and refresh token.

**Activate OAuth**
By default, the OAuth 2.0 (com.snc.platform.security.oauth) plugin is active on new and upgraded instances. If the plugin is not active on your instance, you can activate it.

Role required: admin
1. Navigate to System Applications > All Available Applications > All.
2. Find the plugin using the filter criteria and search bar.
   You can search for the plugin by its name or ID. If you cannot find a plugin, you might have to request it from ServiceNow personnel. For more information, see Request a plugin.
3. Click Install, and then in the Activate Plugin dialog box, click Activate.

**Note:** When domain separation and delegated admin are enabled in an instance, the administrative user must be in the global domain. Otherwise, the following error appears: Application installation is unavailable because another operation is running: Plugin Activation for <plugin name>.

**Set the OAuth property**
To generate OAuth 2.0 tokens to registered applications, the com.snc.platform.security.oauth.is.active property must be active for the instance.

Role required: admin
1. To use OAuth 2.0, enter sys_properties.list in the Workspace filter navigator and click New.
2. Fill out the form with the following settings:
   • Name: com.snc.platform.security.oauth.is.active
   • Type: true | false
   • Value: true

**Create an endpoint for clients to access the instance**
Create an OAuth application endpoint for external client applications to access the ServiceNow instance.

Role required: admin
1. Navigate to System OAuth > Application Registry and then click New.
2. On the interceptor page, click Create an OAuth API endpoint for external clients and then fill in the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Client ID</td>
<td>[Read-Only] The auto-generated unique ID of the application. The instance uses the client ID when requesting an access token.</td>
</tr>
<tr>
<td>Client Secret</td>
<td>[Required] The shared secret string that both the instance and the client application or website use to authorize communications with one another. The instance uses the client secret when requesting an access token. Leave this field blank to have the instance auto-generate a client secret. To display existing client secrets, click the lock icon.</td>
</tr>
<tr>
<td>Redirect URL</td>
<td>The callback URL that the authorization server redirects to. Enter the full URLs of the clients requesting access to the resource, appended by /oauth_redirect.do. For example, http://token_consumer:port/oauth_redirect.do. Enter as many URLs as needed for all possible token consumers. The instance matches the URL of the incoming request to one of the redirect URLs. If no match is made, the instance uses the first redirect URL.</td>
</tr>
<tr>
<td>Logo URL</td>
<td>The URL that contains an image to use as the application logo. The logo appears on the approval page when the user receives a request to grant a client application access to a restricted resource on the instance.</td>
</tr>
<tr>
<td>Active</td>
<td>Select the check box to make the application registry active.</td>
</tr>
<tr>
<td>Refresh Token Lifespan</td>
<td>The number of seconds that a refresh token is valid. The instance uses the lifespan value when requesting a refresh token. By default, refresh tokens expire in 100 days (8640000 seconds).</td>
</tr>
<tr>
<td>Access Token Lifespan</td>
<td>The number of seconds that an access token is valid. The instance uses the lifespan value when requesting an access token. By default, access tokens expire in 30 minutes (1800 seconds).</td>
</tr>
<tr>
<td>Comments</td>
<td>Additional information to associate with the application.</td>
</tr>
</tbody>
</table>

3. Click **Submit**. The record is saved in the Application Registries [oauth_entity] table.

The system creates a record in the Application Registries [oauth_entity] table with of type **OAuth Client**. When the instance actually issues tokens and authorization codes, they are stored in the table. See for more information.

**Configure an OAuth OIDC provider on the Now Platform**

You can configure an OAuth OIDC provider to accept identity tokens generated by a third-party OIDC provider using inbound API calls or our Single Sign-On option (Multi-Provider SSO).

Role required: admin
The Now Platform supports OIDC through our external Single Sign-On (SSO) implementation in addition to inbound API calls. For an example of an OIDC provider configuration, see setting up Azure AD. For an SSO-specific example of an OIDC provider configuration, see Create an OpenID Connect (OIDC) configuration for Single Sign-On (SSO).

1. Navigate to **System OAuth > Application Registry**
   - Click **New**, click **Configure an OIDC provider to verify ID tokens**, and then fill in the form.
   - Select an existing template for an OIDC provider (ADFS, Auth0, Azure AD, Google, Okta), and then fill in the form.

**Note:** OIDC provider templates are available after loading demo data with the OAuth 2.0 plugin.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name that identifies the OAuth OIDC entity.</td>
</tr>
<tr>
<td>Client ID</td>
<td>The client ID of the application registered in the third-party OAuth OIDC server. The instance uses the client ID when requesting an access token.</td>
</tr>
<tr>
<td>Client Secret</td>
<td>The client secret of the application registered in the third-party OAuth OIDC server.</td>
</tr>
<tr>
<td>OAuth API Script</td>
<td>A script you can use to customize requests and responses to an external OAuth provider.</td>
</tr>
<tr>
<td>OAuth OIDC Provider Configuration</td>
<td>The OIDC provider (ADFS, Auth0, Azure AD, Google, Okta) you can use to validate the JWT token. Click the record of your OIDC provider configuration to validate the <strong>User Claim</strong> and <strong>User Field</strong> are set appropriately. If you check <strong>Enable JTI claim verification</strong>, the ServiceNow JWT token validation also validates the JTI sent by the provider.</td>
</tr>
<tr>
<td>Clock Skew</td>
<td>The number, in seconds, for the constraint to be considered valid. The default is 300.</td>
</tr>
<tr>
<td>Comments</td>
<td>Additional information to associate with the application.</td>
</tr>
<tr>
<td>Application</td>
<td>The name of the application containing this entity.</td>
</tr>
<tr>
<td>Accessible from</td>
<td>Select an option to make it accessible from all application scopes, or this application scope only.</td>
</tr>
<tr>
<td>Active</td>
<td>Select the check box to make the OAuth application active.</td>
</tr>
<tr>
<td>Redirect URL</td>
<td>The URL of the OAuth application for receiving the authorization code.</td>
</tr>
<tr>
<td>End Session Endpoint URL</td>
<td>The URL endpoint which enables after a session ends.</td>
</tr>
<tr>
<td>Enable force authentication</td>
<td>Option to enable force authentication for users.</td>
</tr>
</tbody>
</table>
2. Click **Submit**. The record is saved in the Application Registries [oauth_entity] table. The system creates a record in the Application Registries [oauth_entity] table with type **External OIDC Provider**. When the instance actually issues tokens and authorization codes, they are stored in the table. See for more information.

3. Optional: Go to the related list on the record OAuth Entity Profiles to validate a system generated default profile for the new OAuth provider without any scope. You can change or add an OAuth provider profile including the name, grant type, and OAuth Scope.

4. Optional: Go to the related list on the record OAuth Entity Scopes to define all available OAuth scopes for this OAuth provider. The scopes defined can be selected when you create or update a profile. Each OAuth scope defined contains a name and a scope that you must get from the provider specification, such as a read-scope or a write-scope. Each scope must be defined separately.

5. Optional: Go to the related list on the record User Provisioning to enable automatic user provisioning.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Automatically provision users</strong></td>
<td>Option to enable force authentication for users.</td>
</tr>
<tr>
<td><strong>Provision data source</strong></td>
<td>The data source to use to transform an OIDC token to a ServiceNow user. Use the <strong>Lookup list</strong> to select the pre-defined data source template, then open the record to configure the Transforms table mapping. When configuring the Transform mapping, the source fields are from the <strong>JWT token</strong>, the target fields are from the <strong>sys_user</strong> table.</td>
</tr>
<tr>
<td><strong>User roles applied to provisioned users</strong></td>
<td>The user roles applied to the newly provisioned ServiceNow users.</td>
</tr>
</tbody>
</table>

**Connect to a third-party OAuth provider**

Configure how the client ID and secret are sent to your OAuth provider.

Role required: admin

1. Navigate to System OAuth > Application Registry and then click **New**.
2. On the interceptor page, click **Connect to a third-party OAuth provider** and then fill in the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name for the third-party OAuth connection.</td>
</tr>
<tr>
<td>Client ID</td>
<td>The client ID of application registered in the third-party OAuth server.</td>
</tr>
<tr>
<td>Client Secret</td>
<td>The client secret of the application registered in the third-party OAuth server.</td>
</tr>
<tr>
<td>OAuth API Script</td>
<td>The script used to customize request and response to the external OAuth provider.</td>
</tr>
<tr>
<td>Logo URL</td>
<td>The OAuth application logo URL.</td>
</tr>
<tr>
<td>Default Grant type</td>
<td>The default grant type used to establish the token. Choices include:</td>
</tr>
<tr>
<td></td>
<td>• Authorization Code</td>
</tr>
<tr>
<td></td>
<td>• Resource Owner Password Credentials</td>
</tr>
<tr>
<td></td>
<td>• Client Credentials</td>
</tr>
<tr>
<td></td>
<td>• JWT Bearer</td>
</tr>
<tr>
<td>Refresh Token Lifespan</td>
<td>Time, in seconds, that the refresh token is valid. The default time is 8,640,0000 seconds.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>PKCE required</td>
<td>Enables public clients to require PKCE for an authorization.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You can use only Authorization Code as the Default Grant type when PKCE is enabled.</td>
</tr>
<tr>
<td>Code challenge method</td>
<td>The code challenge method used in OAuth PKCE workflow. Choices include:</td>
</tr>
<tr>
<td></td>
<td>•  S256 [Default]</td>
</tr>
<tr>
<td></td>
<td>•  Plain</td>
</tr>
<tr>
<td></td>
<td>•  None</td>
</tr>
<tr>
<td>Comments</td>
<td>Add any comments regarding the OAuth app.</td>
</tr>
<tr>
<td>Application</td>
<td>Application and scope that contain this record.</td>
</tr>
<tr>
<td>Accessible from</td>
<td>Make this app accessible from all application scopes or from this scope only.</td>
</tr>
<tr>
<td>Active</td>
<td>Select the check box to make the app active.</td>
</tr>
<tr>
<td>Authorization URL</td>
<td>The OAuth authorization code endpoint.</td>
</tr>
<tr>
<td>Token URL</td>
<td>The OAuth server token endpoint.</td>
</tr>
<tr>
<td>Token Revocation URL</td>
<td>The OAuth server token revocation endpoint.</td>
</tr>
<tr>
<td>Redirect URL</td>
<td>The OAuth callback endpoint. If blank, the instance auto-generates an entry.</td>
</tr>
<tr>
<td>Use mutual authentication</td>
<td>Check the box to use mutual authentication for token request and revocation. This feature requires a mutual authentication profile to be specified.</td>
</tr>
<tr>
<td>Send Credentials</td>
<td>The OAuth client populates the client credentials in the request:</td>
</tr>
<tr>
<td></td>
<td>•  In Request Body (Form URL-Encoded)</td>
</tr>
<tr>
<td></td>
<td>•  Basic Authorization header</td>
</tr>
</tbody>
</table>

The system creates a record in the Application Registries [oauth_entity] table with type **OAuth Provider**.

3. Optional: Go to the related list on the record OAuth Entity Profiles to validate a system-generated default profile for the new OAuth provider without any scope.
   You can change or add an OAuth provider profile including the name, grant type, and OAuth Scope.

4. Optional: Go to the related list on the record OAuth Entity Scopes to define all available OAuth scopes for this OAuth provider. You can select the scopes when you create or update a profile.
   Each OAuth scope contains a name and a scope that you must get from the provider's specification, such as a read scope or a write scope. Each scope must be defined separately.

*Change OAuth password parameter*

Use this property to insure only POST body parameters are accepted as input for all supported grant types.

Sending sensitive information over URI query parameters might lead to sensitive information disclosure by clients, the server, or any host between the requests. Starting with the Madrid release, this new property insures only the POST body parameters are accepted as input for all supported grant types. Supported grant types include:

- authorization code
• password
• client credential
• refresh token

**OAuth password parameter property**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.oauth.allow.parameters.in.post.body.only</td>
<td>This property is set to true for zBoots only, as part of the OAuth 2.0 plugin. If you need this setting for your instance, create and set the property to true.</td>
</tr>
</tbody>
</table>

**OAuth parameters for default profile support**

The default profile feature requires a set of parameters that you can use with the `setParameter()` API to specify the OAuth requestor, a context for the request, and the provider profile.

In the OAuth provider scenario, you must set three parameters that tell the OAuth provider which OAuth profile to use by default. When these three parameters are set, the access token is saved in the instance database. Use the parameters with `GlideOAuthClientRequest`.

**OAuth parameters for default profile support**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>oauth_requestor</td>
<td>The sys_id of the object, which can be a user record or an email account.</td>
</tr>
<tr>
<td>oauth_requestor_context</td>
<td>Descriptor that provides context for the OAuth requestor. As a good practice, use the name of the table where the <code>oauth_requestor</code> object is saved.</td>
</tr>
<tr>
<td>oauth_provider_profile</td>
<td>The sys_id of the OAuth profile record that is the default (see Specify an OAuth profile).</td>
</tr>
</tbody>
</table>

You do not need to use parameters to set the grant type and scope because the values are configured in the OAuth profile record. If you do not use the parameters, you can use the `GlideOAuthClientRequest` methods `setScope` and `setGrantType`. For additional information, see `setScope` and `setGrantType`.

**OAuth API request parameters**

Access token requests use the following request parameters.

**Note:** The content-type of the OAuth API should be application/x-www-form-urlencoded. A content-type of application/json results in an unspecified error.
### Access token request parameters

<table>
<thead>
<tr>
<th>Request parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| grant_type        | [Required] The type of credentials authorizing the request for an access token. This parameter must have one of the following values:  
> • **password**: A set of user credentials authorize the access token request. Specify the user credentials in the username and password parameters.  
> • **refresh_token**: An existing refresh token authorizes the access token request. Specify the refresh token in the refresh_token parameter. |
| client_id         | [Required] Auto-generated unique ID of the client application requesting the access token. |
| client_secret     | [Required] Shared secret string that the instance and the OAuth application use to authorize communications with one another. |
| username          | User account name that authorizes the access token request. This parameter is required for access token requests with a grant_type of password. |
| password          | Password for the user account that authorizes the access token request. This parameter is required for access token requests with a grant_type of password. |
| refresh_token     | Existing refresh token that authorizes the access token request. This parameter is required for access token requests with a grant_type of refresh_token. |

### Requests Using User Credentials

The instance requires clients to provide user login credentials when first authorizing the client or when authorizing the creation of a new refresh token. This type of request always returns two tokens:  
- An access token  
- A refresh token

The instance verifies that the user is active, not currently locked out, and has an interactive session. If any of these conditions are false, the instance does not produce an access token. Access requests made within the expiration time of the access token always return the current access token.

**Note:** This type of authorization grant relies on TLS encryption to protect the user credentials during transmission.

The following example illustrates requesting an access token with a set of user credentials. (Spaces have been added to improve readability.)

```
$ curl -d"grant_type=password&client_id=be3aeb583ace210011c15b24a43e25d8&client_secret=client_password&username=admin&password=admin"
```
Requests Using a Refresh Token

The instance can use an existing refresh token to create a new access token. This type of request returns only an access token. The instance confirms that the refresh token has not expired before generating a new access token. Access requests made within the refresh token expiration time always return the current refresh token. Transmitting refresh tokens is generally more secure than transmitting user credentials. The following example illustrates requesting an access token with an existing refresh token. (Spaces have been added to improve readability.)

```
$ curl -d "grant_type=refresh_token&client_id=be3aeb583ace210011c15b24a43e25d8 &client_secret=client_password &refresh_token=w599voG89897rGVDmdp12WA681r9E5948c1CJTPi8q4HGc4NWaz62k6k1K0FMxHW40H8y0O3Hoe"
https://instancename.service-now.com/oauth_token.do
```

OAuth API response parameters

The OAuth 2.0 API produces a JSON response containing the following parameters as name:value pairs.

### Access token response parameters

<table>
<thead>
<tr>
<th>Response parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scope</td>
<td>Amount of access granted by the access token. The scope is always <strong>useraccount</strong>, meaning that the access token has the same rights as the user account that authorized the token. For example, if Abel Tuter authorizes an application by providing his login credentials, then the resulting access token grants the token bearer the same access privileges as Abel Tuter.</td>
</tr>
<tr>
<td>token_type</td>
<td>Type of token issued by the request as defined in the OAuth RFC. The token type is always <strong>Bearer</strong>, meaning that anyone in possession of the access token can access a protected resource without providing a cryptographic key. See RFC6750 for more information about how OAuth 2.0 uses bearer tokens.</td>
</tr>
<tr>
<td>expires_in</td>
<td>Lifespan of the access token in seconds.</td>
</tr>
<tr>
<td>refresh_token</td>
<td>String value of the refresh token.</td>
</tr>
<tr>
<td>access_token</td>
<td>String value of the access token. Access requests made within the access token expiration time always return the current access token.</td>
</tr>
<tr>
<td>format</td>
<td>[Optional] Output format of the response. This value is always JSON.</td>
</tr>
</tbody>
</table>

The following example illustrates the JSON string returned by an access token request. (Spaces have been added to improve readability.)

```
{"scope":"useraccount","token_type":"Bearer","expires_in":1800,"refresh_token":"w599voG89897rGVDmdp12WA681r9E5948c1CJTPi8q4HGc4NWaz62k6k1K0FMxHW40H8y0O3Hoe"}
```
OAuth authorization code grant flow

Authorization code grant flow allows a user to access a resource by authenticating directly with an OAuth server that trusts the resource, in contrast with authenticating with username/password credentials.

This implementation of OAuth authorization code flow allows access to a resource via REST. The authorization code framework gets the access token through the authorized URL that the user configures rather than requiring the user to enter a username/password. The username/password are never exposed to the client that is requesting access to the resource.

A ServiceNow instance as the authorization server

The OAuth server is typically a third-party authorization server. You can also specify a ServiceNow instance as the authorization server that issues the tokens for authorization code flow.

The user who owns the restricted resource must authorize access. The user can also revoke the issued access token at any time to terminate access.

Authorization code grant flow process

The Authorization code grant flow process consists of these three steps:

1. **Initial token request**
   - The client application or website initiates a REST API call in the form of a GET request to the instance via the user agent. Typically, the REST call is initiated when the end user clicks a button or a link on the client application or website to request an access token. In the client application, the end user also has to specify the authorization URL, token URL, client ID, and client secret. For an explanation of these items, see the field descriptions in this topic: Use a third-party OAuth provider. If the client asks for a grant type, the end user must select **Authorization Code**.
   
   Example GET request from the client application to the instance:
   
   ```
   https://myinstance.servicenow.com/oauth_auth.do?
   response_type=code&redirect_uri={the_redirect_url}&client_id={the_client_identifier}
   ```
Note: The response_type must be code to use the standard OAuth code grant flow.

The end user must manually allow access to the restricted resource on the instance. In the ServiceNow implementation, the end user must be logged into the instance. The instance prompts the end user with a UI page that has Allow and Deny buttons. See for instructions.

The item that the client application is actually requesting the token from is the OAuth provider application registry record that you created, also known as the authorization endpoint (see Use a third-party OAuth provider). The auth code is sent from the authorization endpoint to the client. It does not go to the client directly but to the Redirect URL that you specify on the authorization endpoint form. This URL is also known as a callback URL. You can obtain this URL from the client application or website.

Example response from the instance to the client application, providing an authorization code:

```
https/http://{callbackURL}?code={the actual auth code}
```

Now that the client application has the authorization code, the client uses the code to request the access token. The authorization code proves that the user has consented in step 1.

Example POST request from the client application to the ServiceNow instance that provides the auth code and requests the access token:

```
https://myinstance.servicenow.com/oauth_token.do?grant_type=authorization_code&code={the auth code}&redirect_uri={the_same_redirect_url}&client_id={the_same_client_identifier}&client_secret={client_secret_value}
```

The endpoint on the instance returns an access token and a refresh token. The refresh token can be used to request additional access tokens.

You can manage the tokens, including revoking the token, in the instance. See .
The client application uses the access token to authenticate to the REST API. After authenticating the client application, the REST API returns the requested data in a JSON payload.

Example GET request for the JSON payload of data for the Incident [incident] table:

```
https://myinstance.service-now.com/api/now/table/incident?
access_token={the_token}
```

**Note:** The system also supports, also known as implicit grant code flow.

### Integration support

Authorization code flow supports the following integrations on the instance:

- Multi-S SO
- SAML 2.0 Update 1
- Multifactor authentication

The mobile interface is also supported.

**OAuth implicit grants**

ServiceNow instances support the implicit grant of an access token.

The implicit grant type, also known as *implicit grant code flow*, allows the access token to be given directly to the client application via the user agent, which is typically the web browser or mobile device. No refresh tokens are granted. The end user must still grant access to the protected resource on the instance, just as with standard.

**OAuth implicit grant flow process**

Just as with the standard authorization code flow process, the client application makes a request to use the restricted resource on the instance and the end user approves it. The request is in the form of a URL sent to the instance. The URL must include the following parameters:

- `client_id=(the necessary client ID)`. This is **mandatory** to identify which protected resource the client application wants access to.
- `response_type=token`. This is **mandatory** to request the access token directly (as opposed to asking for an authorization code). The value must be `token` for implicit grants. In the standard authorization code flow example, the response type is `code`.
- `redirect_uri=[a URL]`: The location where the token is sent.
The authorization server sends the access token, rather than an authorization code, to client application via the user agent.

Here is an example GET request to receive the JSON payload of data for the Incident [incident] table:

```
https://myinstance.servicenow.com/oauth_auth.do?
response_type=token&redirect_uri={the_redirect_url}&client_id={the_client_identifier}
```

If the user grants access, the token is included in the redirect (callback) URL:

```
https/http://{callbackURL}?access_token={the_token}
```

**Authorize access to an OAuth endpoint using auth code flow**

End users who own a protected resource on the ServiceNow instance must authorize access to the resource before the instance can provide the access token.

You must already be logged in to the instance that holds the protected resource. Alternatively, you can log in using the authentication method (such as multi-factor authentication or SAML) that your ServiceNow administrator already set up.

1. Click the link or button on the client application where you are requesting access to the protected resource on the instance. This kicks off the token request.
   If you are making a REST call from one instance to another, this link is **Get OAuth Token** on the REST Message form.
2. If you are not logged in, log in now. If you are not the same user as the user specified in the upper-right corner, click **Not You?** and log in.
3. Click account permissions to open the list of access tokens that you have already issued. is the same as the **Self-Service > My connected apps** token list.
4. Click **Allow** to allow access and have the instance issue the authorization code (if using auth code flow) or the access token (if using implicit grant type). If you click **Deny**, the authorization is not allowed, but you are not logged out of the instance.

A message that confirms access should appear. If you are requesting access from the REST Message form on an instance, the following message appears at the top of the form: **OAuth Refresh token is available and will expire at {date}**.
Authorization code flow state parameter requirement
The glide.oauth.state.parameter.required system property enables the State parameter to be required in an OAuth request for authorization code flow.

State parameter
Beginning in the Madrid release, the system property glide.oauth.state.parameter.required adds a State parameter for an OAuth request. For zbooted instances, the property is true. For upgraded instances, the property is not present, so the State parameter is not enabled. The State parameter is a string value, and should not contain special characters. The State parameter cannot be empty or “”.

Validating the state parameter
Create an endpoint for clients to access the instance. Initiate an authorization code flow for oauth_auth.do. For example:

```plaintext
http://10.11.95.5:16001/oauth_auth.do?grant_type=authorization_code&client_id=e9dba45b380d1300e676ccc91cef468f&response_type=code
```
If you do not specify the state parameter in the request, you get an error and the authorization code is not returned. Missing State parameter in request.

Adding the State parameter to the request:

```plaintext
http://10.11.95.5:16001/oauth_auth.do?grant_type=authorization_code&client_id=e9dba45b380d1300e676ccc91cef468f&response_type=code&state=123
```
Adding the State parameter redirects you to the login screen and the regular authorization code flow returns the authorization code.

Note: The response URL contains the state parameter passed in the request. In the example, the added parameter is state=123.

If the authorization code flow starts from oauth_initiator.do:

```plaintext
http://10.11.95.5:16001/oauth_initiator.do?oauth_requestor_context=sys_rest_message&oauth_requestor=eab8341fec0d1300964f214a2c2fcf67&oauth_provider_profile=dfa8f01fec0d1300964f214a2c2fcf51&response_type=code
```
The State parameter is automatically added when redirected by oauth_auth.do.

```plaintext
http://10.11.95.5:16001/oauth_auth.do?response_type=code&state=-790938844&redirect_uri=http://10.11.95.5:16001/oauth_redirect.do&client_id=e9dba45b380d1300e676ccc91cef468f
```

Authorization code flow example: ServiceNow instance as authorization server
You can use an instance as an authorization server to issue tokens to a client using authorization code flow. This example uses two instances: one as the authorization server and the other as the client. One instance uses a REST call to request tokens from another instance.

You must Activate OAuth on both instances.

1. On the authorization server instance (running the Istanbul or later release), navigate to System OAuth > Application Registry and then click New.
2. Click Create an OAuth API endpoint for external clients.
3. Fill out the form fields for the OAuth application record as described in Create an endpoint for clients to access the instance.
Completing these steps sets up an authorization server. Follow the next steps to set up the client server.

4. On the client instance, navigate to System OAuth > Application Registry and then click New.

5. Click Connect to a third party OAuth Provider.

6. Fill out the form fields for the OAuth application record as described in Use a third-party OAuth provider.
Note the following field values:
- **Client ID**: Client ID of the application registry record that you created for the authorization server.
- **Default Grant type**: Select Authorization code.
- **Authorization URL**: URL of the instance that is the authorization server. Remember to append oauth_auth.do at the end of the URL.
- **Token URL**: URL of the instance that is the authorization server. Remember to append oauth_token.do at the end of the URL.
- **Redirect URL**: URL of this instance: the client server instance. Remember to append oauth_redirect.do at the end of the URL.

7. Create a profile for the record with the Authorization code grant type.
The client server is setup. You can now create an outbound REST message and get an OAuth token.

8. Navigate to System Web Services > Outbound > REST Message and then click New.

9. Fill out the form fields for the OAuth application record as described in .
Note the following field values:
- **Endpoint**: URL of the instance that is the authorization server.
- **Authentication type**: OAuth 2.0.
- **OAuth profile**: OAuth profile that you created for the client server.

10. On the REST message record, click Get OAuth Token.

11. Authenticate with the instance that provides the token—the method depends on the single-sign on integration. You might use:
- Your username and password that you use to authenticate to the instance.
- The username and password for the IdP if is enabled. Click Use External Login to access the IdP login screen.

    **Note**: In order to automatically get redirected to the IdP login page, you must set the glide.authenticate.external system property.
- Your code, if MFA is enabled.

12. Click Allow or Deny to complete the authorization and issue the tokens.
The process that follows is outlined in OAuth authorization code grant flow.

**Manage OAuth tokens**

Open OAuth tokens to provide access to restricted resources.

Role required: any user or admin

Only the tokens that the instance issues are available, not the tokens that the instance can receive to access third-party resources.

1. Navigate to one of the following menu options:
   - **Self-Service > My Connected Apps** to see the tokens that the instance created when you granted access to a resource on the instance.
• **System OAuth > Manage Tokens** to see all tokens. Only administrators can access this module.

2. Click the **Name** to open the token.
3. Click **Revoke Access** to prevent access to the restricted resource.
4. You can also view other information about the token, including the scope it allows access to and the expiration date.

**Revoke an OAuth token**

You might want to revoke an OAuth access or refresh token for security reasons.

Role required: admin

Revoking the token pertains to the situation where your instance acts as the OAuth resource server. You can revoke the token through a URL or by:

- Access your instance using `oauth_revoke_token.do` and append the access or refresh token.

  For example: `https://[Your_ServiceNow_Instance]:[port]/oauth_revoke_token.do?token=[access or refresh token] without the brackets [ ]`.

This endpoint access does not require authentication. The token in this request is marked as expired.

**Set up OAuth provider with JWT Bearer grant type**

JSON Web Tokens (JWTs) enable the capability to configure server-to-server API interactions between ServiceNow and external API providers without requiring any user intervention. This support enables IntegrationHub or other automated tasks using JWTs to configure API and Service integrations with different providers.

Role required: admin

The following tasks show how ServiceNow can be set up to use JWTs for OAuth 2.0 client authentication and authorization grants. ServiceNow is the OAuth client, and you can configure an OAuth provider, such as Box or Docusign.

1. **Upload Java Key Store certificate**
   - Attach a JKS certificate to your instance to use to enable the JWT client authentication.
2. **Configure a JWT signing key**
   - Create a JWT signing key to assign to your Java KeyStore (JKS) certificate.
3. **Create a JWT provider with a JWT signing key**
   - Add a JWT provider to your ServiceNow instance.
4. **Connect to a third-party OAuth provider**
   - Create a third-party OAuth provider with a JWT Bearer as the default grant type in the ServiceNow Application Registry.
5. **Specify an OAuth profile**
   - Open the OAuth entity profile of the OAuth provider and assign a JWT provider.

**Upload Java Key Store certificate**

You can attach a Java KeyStore (JKS) certificate to your instance to use to enable the JWT client authentication.

Role required: admin

1. Navigate to Multi-Provider SSO > x509 Certificate.
2. Fill in the form and click **Submit**:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name for your certificate.</td>
</tr>
<tr>
<td>Notify on expiration</td>
<td>Designate whom to notify when the certificate expires.</td>
</tr>
</tbody>
</table>
### Configure a JWT signing key

Create a JSON Web Token (JWT) signing key to assign to your Java KeyStore (JKS) certificate,

Role required: admin

1. Navigate to **System OAuth > JWT Keys**.
2. Fill in the form and click **Submit**:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name for your JWT Key signing configuration.</td>
</tr>
<tr>
<td>Signing Keystore</td>
<td>The keystore designated when signing the JWT.</td>
</tr>
<tr>
<td>Key ID</td>
<td>The Key ID (kid) helps identify which key is used when multiple keys are used to sign tokens.</td>
</tr>
</tbody>
</table>

**Note:** If you configure this field, the Key ID claim is included in the JWT. If you do not configure this field, your JWT will not have a Key ID claim.

<table>
<thead>
<tr>
<th>Signing Algorithm</th>
<th>The algorithm to use to sign with the JWT key. RSA 256 is the only algorithm available.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signing Key Password</td>
<td>The password associated with the signing key.</td>
</tr>
<tr>
<td>Active</td>
<td>Designate that the JWT key alias is actively referenced from a JWT provider.</td>
</tr>
</tbody>
</table>

### Create a JWT provider with a JWT signing key

Add a JSON Web Token (JWT) provider to your ServiceNow instance.

Role required: admin

1. Navigate to **System OAuth > JWT Provider**.
2. Fill in the form and click **Submit**:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name for your JWT provider configuration.</td>
</tr>
<tr>
<td>Expiry Interval (sec)</td>
<td>The lifespan of the tokens, in seconds, generated by the JWT provider.</td>
</tr>
<tr>
<td>Signing Configuration</td>
<td>The ServiceNow JWT signing key configuration to apply.</td>
</tr>
</tbody>
</table>

### Generate a JSON Web Token (JWT)

Create a JSON Web Token (JWT) for representing claims securely between two parties on the Now Platform.
The GlideJWT API is a scoped, scriptable API which generates a JWT. There are three arguments necessary before generating the JWT:

- **Sys_id of JWT Provider**
- **JSON serialized header**
- **JSON serialized payload**

There are two JWT API scripts, JWTTokenInternal and JWTTokenRestricted, that you can use when configuring a JWT Provider. The JWTTokenRestricted script enables administrators to configure who can generate a JWT. The JWTTokenInternal script is read-only and enables only logged in users to generate a JWT.

To generate a JWT:

- **Create a JWT Key with a shared key (HMAC) or a signing keystore (RSA)**
- **Associate a JWT provider with the signing configuration referring a JWT key**

You can use the API to create your token. You can use standard and custom claims when configuring a JWT provider. You can pass dynamic header and payload claims as part of the generateJWT API signature.

Sample script to test API:

```javascript
var jwtAPI = new sn_auth.GlideJWTAPI();
var headerJSON = {  "kid": "a1234"  };
var header = JSON.stringify(headerJSON);

var payloadJSON = {  "jti": "testjti",  "iss": "testiss",  "sub": "testsub"  };
var payload = JSON.stringify(payloadJSON);

var jwtProviderSysId = "7a40dde2d5303300964fb7c8f3c14ab5";
var jwt = jwtAPI.generateJWT(jwtProviderSysId, header, payload);

gs.info("JWT:" + jwt);
```

**OAuth client APIs**

The OAuth client API provides methods to request and revoke OAuth tokens. The OAuth client provides these classes:

- **GlideOAuthClient**: Methods for requesting and revoking the refresh and access tokens.
- **GlideOAuthClientRequest**: Methods for handling client requests.
- **GlideOAuthClientResponse**: Methods for handling client responses.
- **GlideOAuthToken**: Methods for retrieving the access token and information about the access token.

You can also customize the OAuthUtil script include to intercept the request parameters and also parse the responses from external OAuth providers.

When using OAuth classes in a scoped script, use the `sn_auth` namespace identifier.

**Scoped OAuth APIs**

OAuth supports application scoping by providing access to all OAuth methods in the available OAuth classes using the `sn_auth` namespace identifier.

For example, the following code accesses the requestToken:
var OAuthClient = new sn_auth.GlideOAuthClient();
var tokenResponse = OAuthClient.requestTokenByRequest('TestClient', text);

When using these methods in the global scope, omit the `sn_auth` namespace identifier.

**Digest token authentication**

The digest token authentication passes user credentials and a digest token within an unencrypted HTTP header.

The instance reads the HTTP header value and compares its computed hash value of the digest token. If the computed hash value matches the digest token value, then the instance searches for a matching value in the User table. If there is a matching value in the User table, the instance considers the user pre-authenticated and logs the user in.

Digest token authentication is more secure than simple unencrypted HTTP headers because any accidental or intentional change to the unencrypted HTTP header produces a different hash value. If the hash value fails to match, the instance denies the user access to the requested instance. This prevents users from attempting to login with another user's credentials.

**Integration requirements**

A Digest Token Authentication integration requires:

- A web server
- SiteMinder or another single sign-on application to pre-authenticate the user on the local network
- A web page or portal that passes user credentials to the target instance in one of these formats
  - HTTP Header
  - URL parameter
  - Cookie
- A web page or portal that creates and passes a digest token to the target instance using one of these encoding techniques
  - SHA1
  - MD5

**Set up Digest Token Authentication**

Setting up digest token authentication involves generating an unencrypted HTTP header and token, then enabling an installation exit and configuring properties.

*Generate an unencrypted HTTP header*

The first step in setting up digest token authentication is to generate an unencrypted HTTP header.

Role required: admin

The system only accepts one HTTP header as the source of pre-authentication.

1. Choose an HTTP header that matches data from the User (sys_user) table.
2. Configure your single sign-on software or authentication portal to generate the desired HTTP header.

For example, here are some sample SiteMinder HTTP headers.

**Sample SiteMinder HTTP headers**

<table>
<thead>
<tr>
<th>User credential</th>
<th>Sample HTTP header</th>
<th>Matching sys_user field</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>SM_USER</td>
<td>user_name</td>
</tr>
</tbody>
</table>
Generate a digest token
After generating an unencrypted HTTP header, generate a digest token for authentication.

Role required: admin

The system only accepts one HTTP header as the source of pre-authentication.

Configure your single sign-on software or authentication portal to generate an HTTP header to contain the digest token.

For example, here is a sample SiteMinder HTTP header.

```
Sample SiteMinder HTTP headers

<table>
<thead>
<tr>
<th>Sample HTTP header</th>
<th>Sample digest HTTP header</th>
<th>Sample HTTP headers with digest</th>
</tr>
</thead>
<tbody>
<tr>
<td>SM_User</td>
<td>DE_USER</td>
<td>SM_USER=joe.employee;DE_USER=K1Nr4lht86b9gEfcoiT0dU/=YLM0=</td>
</tr>
</tbody>
</table>
```

Typically, the authentication portal or web page runs the code to generate a digest token from the unencrypted HTTP header and includes the digest token in the URL to the target instance. See SNC Guru for code samples of generating a digest token.

Enable digest installation exit script
After generating a digest token for authentication, enable a digest installation exist script.

Role required: admin

The system uses an installation exit to identify and decode incoming digest tokens. By default, the installation exit uses SHA1 to compute a hash value.

1. Navigate to System Definition > Installation Exits.
2. Click DigestSingleSignOn.
3. Set Active to true.
4. Click Update.
5. To use MD5 for computing the digest token hash value, change this line: `var MAC_ALG ="HmacSHA1";` to this: `var MAC_ALG ="HmacMD5";`

Enter single sign-on system properties
After enabling a digest installation exist script, configure properties for single sign-on.

Role required: admin

If you are configuring digest token for multi-provider SSO, skip this step and enter the digest properties for multi-provider single sign-on. Set these properties to enable single sign-on with an unencrypted HTTP header.

1. Navigate to System Properties > Single Sign-on.
2. For Enable external authentication, select Yes.
3. For HTTP header name to look for an externally authorized user (e.g. for SiteMinder), enter the HTTP header you generated. For example, SM_USER.
4. For **HTTP header name to look for an externally authorized user (e.g. for Digest Encryption)**, enter the HTTP header you generated. For example, `DE_USER`.

5. For **Service-now.com field name to match against the incoming header**, enter the `sys_user` field that contains matching data. For example, `user_name`.

6. For **Secret passphrase for single sign-on (SSO) encryption/decryption**, enter the secret key (password) to use for encoding digest keys. For example, `SecretKey123`.

7. Click **Save**.

---

**Enter the digest properties for multi-provider single sign-on (SSO)**

After enabling a digest installation exist script, configure properties for multi-provider SSO.

Role required: admin

If you are not using multi-provider single sign-on, configure standard single sign-on properties.

1. Navigate to **Multi-Provider SSO > Identity Providers**.
2. Fill in the fields of Digest Properties form.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the digest token.</td>
</tr>
<tr>
<td>User</td>
<td>Enter the <code>sys_user</code> field that contains the matching data for the incoming header.</td>
</tr>
<tr>
<td><strong>HTTP Digest header name</strong></td>
<td>Enter the HTTP header you generated. For example, <code>DE_USER</code>.</td>
</tr>
<tr>
<td><strong>HTTP header name</strong></td>
<td>Enter the HTTP header you generated for your created digested token. For example, <code>SM_USER</code>.</td>
</tr>
<tr>
<td><strong>Secret Passphrase</strong></td>
<td>Enter the secret key to use for encoding digest keys. For example, <code>SecretKey123</code>.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Failed SSO Redirect field</td>
<td>Enter the URL to redirect users after a failed authentication.</td>
</tr>
<tr>
<td>External logout redirect</td>
<td>Enter the URL to redirect users after a logout.</td>
</tr>
<tr>
<td>Single Sign-on Script</td>
<td>Select MultiSSO_DigestedToken.</td>
</tr>
</tbody>
</table>

3. Click **Update**.

4. Set your Digest Token default to true.

When you set the default to true, this overwrites the system default digest token record associated to SSO. Once the first multi-provider SSO related IdP record activates, only records associated to multi-provider SSO will be used.

Digest token records which exist in digest properties table can be individually called by appending the `Sys_ID` of the IdP. For example, a digest token record in the following authentication URL:

```plaintext
```

**Test the integration**

This single sign-on method allows pre-authentication from URL parameters, HTTP headers, or cookies.

Role required: admin

- Verify users can sign-on from all methods.

For example:

- **URL Format**: `https://<instance_name>.service-now.com?SM_USER=joe.employee&DE_USER=KfNr4nlt86b9EfcoiT0dU/YLM0=
- **HTTP Header Format**: `SM_USER=joe.employee;DE_USER=KfNr4nlt86b9EfcoiT0dU/YLM0=
- **Cookie Format**: `'SM_USER=joe.employee; DE_USER=KfNr4nlt86b9EfcoiT0dU/YLM0="; expires=Fri, 27 Jul 2012 02:47:11 UTC; path=/`

**Create links for digest authentication**

After you set up digest token authentication, construct URLs to take users to a particular page or resource.

Role required: admin

- Create a URL to your instance and append the appropriate user (SM_USER) and digest (DE_USER) request parameters.

Example URLs are as follows:

```
https://demo.service-now.com/nav_to.do?uri=ess&SM_USER=itil&DE_USER=nqQ82LONE=YQnXpmqddxnsvsArrQ=
```

```
https://demo.service-now.com/nav_to.do?uri=incident.do?sys_id=9d385017c611228701d22104cc95c371&SM_USER=itil&DE_USER=Uj/HopjjPczCNPnN2xcCX17kQty4=```

```
http://demo.service-now.com/nav_to.do?uri=incident_list.do?sysparm_userpref_module=4dedbac7d0bbf538017a7f13c4a1f257%26sysparm_query=caller_id=javascript:gs.getUserID()^active=true^EQ&SM_USER=itil&DE_USER=Uj/HopjjPczCNPnN2xcCX17kQty4=
```

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Note: If you are using request parameters inside a URI (nav_to.do?uri=), ampersands (&) are encoded as %26.

Sample digest token implementations

Here are several samples of creating a digest token.

Sample digest authentication implementations

<table>
<thead>
<tr>
<th>Digest built with</th>
<th>Secret key value</th>
<th>Hash method</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java</td>
<td>abc123</td>
<td>SHA1</td>
<td>Sample Java Digest Algorithm for Encryption</td>
</tr>
<tr>
<td>C</td>
<td>Value of sharedKey parameter</td>
<td>Value of strEncryptionMethod parameter (SHA1 or MD5)</td>
<td>Sample C</td>
</tr>
</tbody>
</table>

Sample Java digest algorithm for encryption

This Java algorithm illustrates creating a digest token from an HTTP header.

This sample assumes:

- The web server supports Java
- The hash computation method is SHA1
- The secret key value is abc123
- The unencrypted HTTP header name is user_name

Change the Java code to use another hash computation mechanism (such as MD5), change the secret key value, or HTTP header name.

```java
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import sun.misc.BASE64Encoder;

public class DigestTest {
    private static final String MAC_ALG = "HmacSHA1";
    public byte[] getDigest(String acct) {
        try {
            byte[] bkey = fKey.getBytes();
            byte[] data = acct.getBytes();
            Mac mac = null;
            try {
                mac = Mac.getInstance(MAC_ALG);
                mac.init(new SecretKeySpec(bkey, MAC_ALG));
            } catch (Exception e) {
                e.printStackTrace();
            }
            byte[] sig = mac.doFinal(data);
            String signature = new String(sig);
            System.out.println("value:" + acct);
            System.out.println("digested value: " + signature);
            return sig;
        } catch (IllegalArgumentException e) {
            e.printStackTrace();
        }
        return null;
    }
}
```
Sample C

This C class illustrates creating a digest token from three input parameters.

- `strEncryptionMethod` – lists the hash computation method (SHA1 or MD5)
- `message` – lists the value to be converted into a digest token
- `sharedKey` – lists the secret key

This sample assumes:

- The web server supports C
- Other code calls this class and passes the expected parameters

Sample Code

```c
private string digestData(string strEncryptionMethod, string message, string sharedKey ) {
    UnicodeEncoding myUnicodeEncoding = new UnicodeEncoding();
    byte[] messageBytes = System.Text.Encoding.ASCII.GetBytes(message);
    byte[] sharedKeyBytes = System.Text.Encoding.ASCII.GetBytes(sharedKey);
    byte[] hashedMessage;
    string b64SHA1Message;
    if (this.DEBUG) {
        TextBoxMessage.Text = message;
        TextBoxSecret.Text = sharedKey;
    }
    switch ((strEncryptionMethod)) {
        case "SHA1":
            HMACSHA1 hmacsha1 = new HMACSHA1();
            hmacsha1.Key = sharedKeyBytes;
            hashedMessage = hmacsha1.ComputeHash(messageBytes);
            b64SHA1Message = Convert.ToBase64String(hashedMessage);
            if (this.DEBUG) TextBoxDigest.Text = Convert.ToString(hashedMessage);
            break;
        case "MD5":
            HMACMD5 hmacmd5 = new HMACMD5(sharedKeyBytes);
            hashedMessage = hmacmd5.ComputeHash(messageBytes);
            b64SHA1Message = Convert.ToBase64String(hashedMessage);
            if (this.DEBUG) TextBoxDigest.Text = Convert.ToString(hashedMessage);
            break;
    }
    return b64SHA1Message;
}
```
default :
    b64SHA1Message = "Unknown Encryption Method"; break;
}

TextBoxBase64.Text = b64SHA1Message; return b64SHA1Message;

**REST API access policies**

REST API access policies allow you to restrict access to inbound ServiceNow REST APIs based on the authentication type and the specified filter criteria of the access policy. Filter criteria contains filter conditions or queries that are used as policy inputs for an authentication policy. You can configure the default Global Blocking Policy or create a custom API access policy according to your security requirements.

For example, you can create a custom API access policy that allows only OAuth 2.0 authentication type from a specified range of IP addresses. Authentication requests of other authentication types and access requests from IP addresses other than the specified IP addresses are denied.

**Activate REST API access policy**

You can activate the REST API Access Policy plugin (com.glide.rest.policy) if you have the admin role. The application includes demo data and installs related ServiceNow® Store applications and plugins if they are not already installed.

Role required: admin

The following items are installed with REST API Access Policy:

- Plugins: com.glide.auth.profile, com.snc.adaptive_authentication, com.snc.platform.security.oauth
- Tables: sys_api_access_policy, sys_auth_profile_mapping, auth_policy_mapping, inbound_auth_profile, std_http_auth.

For more information, see Adaptive authentication.

1. Navigate to **System Applications > All Available Applications > All**.
2. Find the REST API Access Policy plugin (com.glide.rest.policy) using the filter criteria and search bar.
   - You can search for the plugin by its name or ID. If you cannot find a plugin, you might have to request it from ServiceNow personnel. For more information, see Request a plugin.
3. Click **Install**, and then in the Activate Plugin dialog box, click **Activate**.

   **Note:** When domain separation and delegated admin are enabled in an instance, the administrative user must be in the **global** domain. Otherwise, the following error appears: Application installation is unavailable because another operation is running: Plugin Activation for <plugin name>.

**Create an authentication profile**

Create an authentication profile and add one or more authentication policies to the profile. You can also configure the **ID Token** and **OAuth Token** authentication profiles that are available by default.

Role required: admin

1. Navigate to **System Web Services > API Access Policies > Inbound Authentication Profiles**.
2. Click **New**.
The system displays the message "What kind of authentication profile?"

3. Select **Create standard http authentication profiles**.
4. On the form, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name to identify the authentication policy.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the authentication policy.</td>
</tr>
<tr>
<td>Active</td>
<td>Option to make the authentication policy active.</td>
</tr>
<tr>
<td>Application</td>
<td>Scope of the authentication policy.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of the authentications available. You can select Basic Auth, ID Token, or OAuth.</td>
</tr>
<tr>
<td>OAuth Entity</td>
<td>OAuth Entity profile. This field appears only when ID Token or OAuth is selected from Type.</td>
</tr>
</tbody>
</table>

5. Double-click **Insert a new row**.
6. Select an authentication policy from the list and click the save icon.

**Note:** Do not select Allow Access Policy or Deny Access Policy. These policies are meant only for user logins.

You can add one or more authentication policies for an authentication profile.

**Create REST API access policy**

Create an API access policy and map an authentication profile to restrict the authentication type for a REST API. For example, you can create an API access policy that allows only ID token authentication for a REST API.

- Role required: admin
- Make sure that an authentication profile is created. For more information, see Create an authentication profile.

1. Navigate to **System Web Services > API Access Policies**.
2. Click **New**.
3. On the form, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name of the API access policy.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Active</td>
<td>Option to make the API access policy active.</td>
</tr>
<tr>
<td>REST API</td>
<td>The REST API to which the access policy is applied. For example, Attachment API.</td>
</tr>
<tr>
<td>REST API PATH</td>
<td>API path of the REST API. This field is auto-populated based on the selected REST API. For example, now/attachment.</td>
</tr>
<tr>
<td>HTTP Method</td>
<td>Method used for interacting with the API. This field is auto-populated based on the selected REST API.</td>
</tr>
</tbody>
</table>
| Version        | Version of the API. For example, v1. This field is auto-populated based on the selected REST API.  
                  | **Note:** If you want to create an authentication policy for all versions of a REST API, you must create individual policies for each version. |
| Resource       | Child resource of the REST API. This field is auto-populated based on the selected REST API. For example, /now/attachment |
| Application    | Scope of the application.                                                   |

4. Double-click **Insert a new row**.
5. Select an inbound authentication profile from the list and click the save icon

You can add one or more inbound authentication profiles.

**Filter criteria for APIs**

Filter criteria contains filter conditions or queries that are used as policy inputs for an authentication policy. Policy inputs are used to group one or more filter criteria and define the policy conditions of an authentication policy. For example, an IP Filter Criteria define an IP address in the Classless Inter-Domain Routing (CIDR) format or a range of IP addresses.

You can create filter criteria based on the user's IP address, role, and the user group to which they belong.

**Note:** You also use the filter criteria created from the **Adaptive Authentication** module. For more information, see Adaptive authentication.

**Create IP filter criteria for APIs**

IP filter criteria allows you filter users based on their IP addresses. You can configure an authentication policy to grant or block access to a specific address or range of addresses.

Role required: admin

1. Navigate to **System Web Services > API Access Policies > Filter criteria**.
2. Click **New**.
   - The system displays the message **What kind of Policy Input (Filter Criteria) do you want to create?**
3. Select **IP Filter Criteria**.
4. On the form, fill in these fields.
### IP Filter Criteria form

<table>
<thead>
<tr>
<th>Filed</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name to identify the IP network.</td>
</tr>
<tr>
<td>Description</td>
<td>Short description of the IP network.</td>
</tr>
<tr>
<td>Application</td>
<td>Scope of the application.</td>
</tr>
</tbody>
</table>

5. Right-click the form header and click **Save**.
6. From the IP Collections tab, click **New**.
The system displays the message **What kind of IP collection do you want to create?**.
7. Select an IP collection.

<table>
<thead>
<tr>
<th>IP Collection</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Range</td>
<td>A range of IPv4 addresses. For example, 192.0.2.0 - 192.0.2.255.</td>
</tr>
<tr>
<td>Subnet</td>
<td>Subnet or subnet mask of an IP network. For example, 255.255.255.0.</td>
</tr>
<tr>
<td>IP Address List</td>
<td>A list of individual IPv4 addresses.</td>
</tr>
</tbody>
</table>

Create an IP collection for APIs
An IP collection can be a range of IP addresses, list of IP addresses or a subnet.
Role required: admin

1. Navigate to **System Web Services > API Access Policies > Filter Criteria**.
2. Open an IP Filter Criteria record.
3. From the **IP Collections** tab, click **New**.
4. Select an IP collection.

<table>
<thead>
<tr>
<th>IP Collection</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Range</td>
<td>A range of IPv4 addresses.</td>
</tr>
<tr>
<td>Subnet</td>
<td>Subnetwork of an IP network.</td>
</tr>
<tr>
<td>IP Address List</td>
<td>A list of individual IPv4 addresses.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>IP Range</strong></th>
<th><strong>IP Address List</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Name</td>
<td>Name to identify the IP range.</td>
</tr>
<tr>
<td>Description</td>
<td>Short description of the IP range.</td>
</tr>
<tr>
<td>Start IP</td>
<td>Starting IP address in a range of addresses. For example, 192.168.0.0</td>
</tr>
<tr>
<td>End IP</td>
<td>Ending IP address for a range of addresses. For example, 192.168.0.24</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Subnet form</strong></th>
<th><strong>IP Address List</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Name</td>
<td>Name to identify the subnet.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Description</td>
<td>Short description of the subnet.</td>
</tr>
<tr>
<td>Network IP</td>
<td>Network IP of the subnet.</td>
</tr>
<tr>
<td>Netmask</td>
<td>Subnet mask or netmask of the subnet.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name to identify the IP address list.</td>
</tr>
<tr>
<td>Description</td>
<td>Short description of the IP address list.</td>
</tr>
</tbody>
</table>

Create role filter criteria for APIs

Role filter criteria allows you to filter users based on roles. You can configure an authentication policy to grant or block access to a list of user roles.

Role required: admin

2. Click New.
   - The system displays the message What kind of Policy Input (Filter Criteria) do you want to create?
3. Select Role Filter Criteria.
4. On the form, fill in these fields.

   **Role Filter Criteria form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name to identify the role.</td>
</tr>
<tr>
<td>Application</td>
<td>Scope of the application.</td>
</tr>
<tr>
<td>Description</td>
<td>Short description of the role.</td>
</tr>
</tbody>
</table>

5. From the Roles for criteria, double-click Insert a new row.
6. Click the search icon
   - look up, and select a role.
7. Click the save icon
   - You can add one or more roles similarly.
8. Add a condition. For more information, see Create a condition statement using the condition

Create group filter criteria for APIs
Group filter criteria allows or denies user access based on the user group to which the user belongs.

Role required: admin

2. Click New.
   The system displays the message What kind of Policy Input (Filter Criteria) do you want to create?
4. On the form, fill in these fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name to identify the group.</td>
</tr>
<tr>
<td>Description</td>
<td>Short description of the group.</td>
</tr>
<tr>
<td>Application</td>
<td>Scope of the application.</td>
</tr>
</tbody>
</table>

5. From the Groups for criteria tab, double-click Insert a new row.
6. Click the search icon

look up, and select a user group.

7. Click the save icon

API Authentication Policies

Authentication policies evaluate authentication requests based on the specified policy conditions and either allows or denies access depending on the matching criteria.

You can use the built-in Global Blocking Policy or create an authentication policy according to your security requirements. Global Blocking Policy denies the authentication requests of users and APIs based on the specified filter criteria.

Note: Do not use or modify Allow Access Policy and Deny Access Policy. These policies are meant only for user logins.

Create an API authentication policy

Authentication policies allow you to enforce access restrictions on the APIs based on the specified filter criteria.

Role required: admin

1. Navigate to **System Web Services > API Authentication Policy**.
2. Click **New**
3. On the form, fill in these fields.

<table>
<thead>
<tr>
<th>Policy form</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>Application</td>
</tr>
</tbody>
</table>

4. Right-click the form header and select **Save**.
5. From the Policy Inputs tab, select **Edit** to add the existing Filter Criteria.
   You can also create a new Policy Input. For more information, see **Create policy inputs**.
6. Move one or more filter criteria from the Collections list to the Policy Inputs

- Add Filter
- Run filter

-- choose field -- ▼  -- oper -- ▼  -- value --

**Collection**

- Blocked IPs
- EMEA Network
- Only Contractors
- Only Employees
- Only Users
- test connection

**Policy Inputs List**

Test Authentication Policy

- APAC Network
- Only Administrators
- **Trusted IPs**

>  <

Name Trusted IPs

Cancel Save
7. Select **Save**.
8. From the Policy Conditions tab, select **New**.
9. On the form, fill in these fields.

**Condition form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>Name of the policy condition.</td>
</tr>
<tr>
<td>Description</td>
<td>Short description of the policy condition.</td>
</tr>
<tr>
<td>Application</td>
<td>Scope of the application.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Condition</td>
<td>One or more conditions that are combined with OR filter.</td>
</tr>
</tbody>
</table>

**Label:** Main Policy Condition  
**Application:** Global

All of the following conditions must be true, for this answer to be used

<table>
<thead>
<tr>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>All of these conditions must be met</td>
</tr>
<tr>
<td>APAC Network ▼ is ▼ true ▼ ✔ OR AND</td>
</tr>
<tr>
<td>or</td>
</tr>
<tr>
<td>All of these conditions must be met</td>
</tr>
<tr>
<td>Only Administrat… ▼ is ▼ true ▼ ✔ OR AND</td>
</tr>
<tr>
<td>or</td>
</tr>
<tr>
<td>All of these conditions must be met</td>
</tr>
<tr>
<td>Trusted IPs ▼ is ▼ true ▼ ✔ OR AND</td>
</tr>
<tr>
<td>or</td>
</tr>
<tr>
<td>New Criteria</td>
</tr>
</tbody>
</table>
10. Select **Submit**.

**Configure global blocking policy for APIs**
Global blocking policy denies the authentication requests of users and APIs based on the specified policy conditions. This policy can be used as an alternative to the IP Address Access Control.

Role required: admin

1. Navigate to **System Web Services > API Access Policies > Global Blocking Policy**.
2. From the **Policy Inputs** tab, click **Edit**.
3. Select one or more filter criteria from the **Collection** list and move them to **Global Blocking Policy** list. You can also add additional filters.
4. From the **Policy Conditions** tab, click **New**.
5. On the form, fill these fields:

<table>
<thead>
<tr>
<th>Condition Form</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Label</td>
<td>Name to identify the condition.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the condition.</td>
</tr>
<tr>
<td>Condition</td>
<td>Logical combination of multiple policy inputs(filter criteria) that is used to evaluate authentication requests. For example, you can create conditions that allow only contractors from a list of trusted IP addresses.</td>
</tr>
</tbody>
</table>

**Multifactor authentication (MFA)**
MFA, also known as two-step verification, is a security requirement that asserts a user enter more than one set of credentials to authenticate to an instance.

The basic level of authentication to an instance is local database authentication where a user enters a username and password combination. MFA gives administrators and users the ability to require a second level of authentication where a user must enter a passcode or token in addition to the password. A mobile application on a user mobile device generates the passcode.

- Users can require MFA for their own login credentials.
- Administrators can require MFA for any user login credentials or specific roles.

**Supported authentication methods**

- You can use MFA with the following authentication methods:
  - Local Database Authentication (native ServiceNow authentication)
  - LDAP integration
Authentication methods that are not supported

- MFA does not support with the following authentication methods:
  - SSO SAML
  - SSO Digest

Administrator MFA authentication flow

**Note:** If a user performs a password change while MFA is enabled on the user profile, the user does not need to enter the authorization code.

1. The administrator goes to a user profile or role in the instances and initiates MFA.
2. The instance displays a QR code and a QC code number.
3. Using a compatible authenticator, scan the QR code with the authenticator, or manually enter the QC code number in the MFA registration screen.
4. A Time-based One-time Password (TOTP) code generates and displays within the authenticator application along with your associated ServiceNow instance name and username.
5. For every subsequent login, enter the TOTP code generated from your authenticator application in the MFA challenge screen that displays after you enter your username and password.
6. If the challenge is correct, the user authenticates to the instance.

You can also skip the MFA challenge screen and directly logon to the instance:

1. You can also append your TOTP code to your password from the initial login screen. If your password is 'XXX' and your TOTP code is '123', you can enter 'XXX123' as your password to skip the MFA challenge screen.
2. If the username, password, and passcode combination are correct, the MFA challenge screen does not appear and the user directly logs into the instance.

MFA FAQs

<table>
<thead>
<tr>
<th>Questions</th>
<th>Answers</th>
</tr>
</thead>
<tbody>
<tr>
<td>What if I do not own a smart phone?</td>
<td>If you do not have access to a smart phone, you can use the Chrome browser Authy extension to set up and use MFA. Download and add the extension to your Chrome browser. Then, set up an Authy account and password with the Chrome extension before you set up MFA with it.</td>
</tr>
</tbody>
</table>
### Questions

<table>
<thead>
<tr>
<th>Questions</th>
<th>Answers</th>
</tr>
</thead>
</table>
| I use Firefox instead of Chrome. Is there an Authy plug-in for Firefox that I can use? | Currently, Firefox does not support the browser-based Authy plug-in. However, you can install the Authy plug-in through the Chrome browser. You can use the Authy app standalone (without using the Chrome browser) for generating the code to use in Firefox to log on to ServiceNow MFA-enabled applications.  

**Note:** After you install Authy, you must select the Multi-Device option from the Devices section. |
| What if I do not have a smart phone while logging in?                     | After the initial pairing, if you do not have your smart phone available, you can email yourself a code to log in.  

| Can I enter the code and my password in one login screen instead of two different screens? | Yes. After initial setup, you can enter your password followed by the 6-digit code in the first login screen to log in. |
| What if I must change devices and re-pair or reenter the code into a different mobile device? | Go to your user profile in the ServiceNow instance under My Profile and click multi-factor authentication to get access to the code to reenter and pair your device. |
| What should I do if my authenticator code obtained from Authy is not working on my computer? | Update the preference on your computer to set the time automatically to generate the correct code. If you manually set the time on your laptop, a time difference could cause the codes to fail. After you sync the time on your laptop, the app confirms that the time syncs and you can use your verification codes to sign in.  

**Note:** The sync only affects the internal time of your authenticator app and does not change the date and time settings on your device. |
| Can I turn it off?                                                        | No, when an administrator enables MFA, a user cannot disable it. |

For help or questions with MFA, contact your ServiceNow administrator.

### Activate the MFA plugin

The Integration - Multifactor Authentication plugin is active by default.

Role required: admin

1. Navigate to **System Applications > All Available Applications > All**.
2. Find the Integration - Multifactor Authentication plugin plugin () using the filter criteria and search bar.
   
   You can search for the plugin by its name or ID. If you cannot find a plugin, you might have to request it from ServiceNow personnel. For more information, see Request a plugin.
3. Click **Install**, and then in the Activate Plugin dialog box, click **Activate**.

**Note:** When domain separation and delegated admin are enabled in an instance, the administrative user must be in the global domain. Otherwise, the following error appears: Application...
Configure multifactor authentication (MFA)

You can enable and customize MFA to meet your security requirements.

To learn more about MFA, see Enable multi-factor authentication (MFA) (instance security hardening) in Instance Security Hardening Settings.

Role required: admin

1. Navigate to **Multi-factor Authentication > Properties**.
2. Configure these properties:

**Multifactor authentication properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Multifactor authentication (glide.authenticate.multifactor)</td>
<td>Option that enables users and administrators to use this feature. The default is enabled. To learn more about this property, see Enable multi-factor authentication (MFA) (instance security hardening) in Instance Security Hardening Settings.</td>
</tr>
<tr>
<td>Number of times a user can bypass multi-factor authentication (glide.authenticate.multifactor.setup.bypass.count)</td>
<td>Number of times that a user can choose to skip the setup of MFA. Your users can still log in to your instance even if they don't have their mobile device with them. If you disable this feature and then reenable it, the counter starts over again. The default is 3.</td>
</tr>
<tr>
<td>The time in minutes the one-time code sent to user's email address is valid for (glide.multifactor.onetime.code.validity)</td>
<td>Number of minutes that the reset code is valid. See Log on with multifactor authentication. The default is 10.</td>
</tr>
<tr>
<td>Additional time in seconds for which the code will be valid to accommodate for the clock skew. The maximum value is 60 seconds. (glide.authenticate.multifactor.clock_skew)</td>
<td>Number of additional seconds that the reset code is valid. The maximum is 60. The default is 10. The instance validates the code entered by the user against the single app-generated code that is generated at the current time. You can skew the time window with this property and allow one or more codes to be generated during a time window to be considered valid. The property’s value is used in the following calculation: current time - x/2 and current time + x/2, where x is the value of this property. If you use the value of 10, for example, the instance considers any codes that are generated by the app between the time range [current time - 5 seconds] and [current time + 5 seconds] to be valid. Use this property to prevent login issues where the user is unable to enter the correct code in the default time allotted.</td>
</tr>
<tr>
<td>Enable remember browser feature for multi-factor authentication.</td>
<td>Set your instance to prompt a user for MFA when they log in from a new device or browser. The default is yes.</td>
</tr>
</tbody>
</table>
3. Click **Save**.

**Tested third-party authenticators with MFA**

Users must install and use an authenticator that supports Time-based One-time Password (TOTP) to generate a temporary MFA passcode.

**Tested third-party authenticators**

Users should install the recommended authenticator to their mobile devices. MFA has been tested with the following authenticators:

- Google Authenticator
- Microsoft Authenticator
- LastPass Authenticator
- Authy
- FreeOTP
- Duo
- Okta Verify

**Note:** Other authenticators not listed might also be compatible.

**Logging into your instance using MFA**

You can log into your instance with your credentials and a generated passcode.

1. Go to your instance login screen and enter credentials.  
   An MFA registration screen displays with a QR code and a QC code number.
2. Using a compatible authenticator, scan the QR code with the authenticator, or manually enter the QC code number in the authenticator application.  
   A TOTP code generates and displays within the authenticator application associated to your ServiceNow instance.
3. For every subsequent login, enter the TOTP code generated from your authenticator application in the MFA challenge screen that displays after you enter your username and password.

**Note:** You can also append your TOTP code to your password from the initial login screen. If your password is ‘XXX’ and your TOTP code is ‘123’, you can enter ‘XXX123’ as your password to skip the MFA challenge screen.

If you properly enter your credentials and current passcode, you should authenticate to the instance.

**Require MFA for a user**

Enable MFA for any user record in the system that you have access to.
Role required: admin

1. Navigate to User Administration > Users.
2. Configure the list to show the Enable Multifactor Authentication column.
3. Change the values of the Enable Multifactor Authentication column for the selected users to true.

When the user logs in with their username and password, they are prompted to set up multifactor authentication.

Enable MFA for high privileged roles

Automatically enable and enforce MFA for users who have high privileged roles that you have access to.

Role required: admin

All users designated with a high privileged role go through MFA before authenticating into the instance. This functionality also makes it easier to administrate MFA for many users based on their roles instead of enabling MFA for them at a per user level.

2. Select Role based multi-factor authentication.
3. Check the Active box.
4. Click Update to save.

When the user with the designated role logs in with their user name and password, they are prompted to set up MFA.
Set up multifactor authentication upon initial login

If your administrator enabled multifactor authentication on your profile but you have not yet set up the application, you can set it up upon login.

Role required: none

1. Log into your instance using your username and password. The multifactor authentication setup screen intercepts your login.

Enable multi-factor authentication

1. Download the Authenticator app for your mobile device
2. Open the app and scan the QR code below to pair your mobile device
3. Enter the code generated by the Authenticator app below

- Apple iTunes
- Google Play
- Windows store

6-digit code

Pair device and Login
2. If you want to skip the authentication setup at this time, click **Bypass Setup**. You can bypass multifactor authentication for a limited number of times that your administrator allows. Eventually you need to configure multifactor authentication.

3. If you do not yet have the Google Authenticator application in your mobile device, you can download it from one of the links provided under **Download the app**.

4. Take a photo of the QC code with the Google Authenticator application or enter the string in the application manually.

5. Enter the code and click **Pair device and log in**.

   The application responds with a six digit code that refreshes every 30 seconds. If you entered the correct code, a message appears telling you that Multifactor Authentication is set up. If you entered an invalid code, look for the code on your mobile device again as it may have refreshed, and enter the code that you see.

   **Note:** For the code to work properly, the system time on your computer must be in the same time zone as the time on your mobile device.

---

Log on with multifactor authentication

After multifactor authentication is enabled for your User profile, you can log in with the addition of the passcode that the Google Authenticator app gives you.

You must have multifactor authentication enabled for your profile. You can enable it yourself on your user profile or your administrator can enable it for you.

Role required: none

1. Go to the URL of your instance to open the log in screen.

2. Open the Google Authenticator application on your mobile device and make note of the number. The number refreshes every 30 seconds.

3. Enter your username and password, and append the passcode that you currently see on your mobile device to your password without any extra spaces. For example, if your password is **12345** and the current passcode is **424 058**, enter **12345424058**.

   If you forget to enter the code and you only enter the password, you are prompted to enter the code in a new window.

4. Enter the code and click **Login**.

5. If you do not remember the passcode, click the **Click to send one-time passcode** link.

   The temporary passcode is sent to your email address. You can append this passcode to your password as you would the original passcode. You can only use this temporary passcode once and it is only valid for 10 minutes.
Note: You must have an email address configured in your user profile on the instance to receive this email message.

Set up multifactor authentication on your own profile

You can set up multifactor authentication on your own User profile.

Role required: none

Note: If you are trying to reset multi-factor authentication, log in to the instance first by requesting the temporary code via email, and then follow the steps below.

1. Navigate to Self-Service > My Profile.
2. Click the Multifactor Authentication related link on your User record.

The multifactor authentication window appears.

Complete the steps below to enable multifactor authentication

1. Download the app
   - Apple iTunes
   - Google Play
   - Windows Store

2. Scan the QR Code:

3. Type in the App’s response:
   - 6 digit response
   - Validate Response
3. If you do not yet have the Google Authenticator application in your mobile device, you can download it from one of the links provided under **Download the app**.

4. Take a photo of the QC code with the Google Authenticator application or enter the string in the application manually.

5. Enter the code and click **Validate Response**.

   The application responds with a six digit code that refreshes every 30 seconds. If you entered the correct code, a message appears telling you that Multifactor Authentication is set up. If you entered an invalid code, look for the code on your mobile device again as it may have refreshed, and enter the code that you see.

   **Note:** For the code to work properly, the system time on your computer must be in the same time zone as the time on your mobile device.

### Disable multifactor authentication on an admin user profile

Only admins can disable multifactor authentication on their own user profile, as long as MFA is not required for the admin role.

**Role required:** admin

1. Log in the instance using your multifactor authentication code appended to your password.
2. Navigate to **Self-Service > My Profile**.
3. Click the **Multifactor Authentication** related link on your User record.
4. Click **Disable Multifactor Authentication**.
5. Confirm the action.

   You return to the user record. The setting is automatically saved. You do not need to save your User record again.

### Disable multifactor authentication on the User table

You can disable multifactor authentication for the users that you have access to on the User table.

**Role required:** admin

1. Log in the instance.
2. Open the User [sys_user] table.
3. Configure the list to show the **Enable Multifactor Authentication** column.
4. Change the values of the **Enable Multifactor Authentication** column for the selected users to **false**.

   These users will no longer need the passcode. However, each user can still enable multifactor authentication for their own user profile. To disable the ability for any user to enable multifactor authentication, **disable the system property**.

### Enable external authentication

You can enable external authentication on your instance.

1. Navigate to **System Definition > Installation Exits**.
2. Activate the **ExternalAuthentication** installation exit.

   **Note:** If you are using the Digest authentication method, you must also enable the **DigestSingleSignOn** installation exit.

3. Navigate to **System Properties > Single Sign-on**.
4. Select **Enable external authentication** and click **Save**.
You can also navigate to the **sys_properties.list** and search for the `glide.authenticate.external` property and set it to True.

Administrators might need to bypass external authentication when testing an SSO integration. Use the following URL to bypass external authentication and log in with a local user: `http://<your-instance>.service-now.com/side_door.do`

- A logged-in user cannot access the page
- Attempting to access the page while logged in produces a 'page not found' error

**Associating custom URLs to your instance**

You can enable your ServiceNow instance to be accessible from a company-branded or custom URL.

**Custom URL overview**

You can configure one or multiple custom URLs to your instance, and configure your custom URL to Service Portal mapping.

**Note:** Custom URLs are not available for on-premise customers or developer instances. Also, the URL must be public-facing.

Only the owner of the top-level domain (TLD) or any subdomain can configure the custom URL to a DNS subdomain. For example, your instance might have the following designated URL and additional custom URLs:

**Custom URL example**

<table>
<thead>
<tr>
<th>Example URLs</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://acme.service-now.com">https://acme.service-now.com</a></td>
<td>The initial domain name for Acme that came with the ServiceNow instance.</td>
</tr>
<tr>
<td><a href="https://support.acme.com">https://support.acme.com</a></td>
<td>A custom URL that associates to your ServiceNow instance. This URL is referred to as an alias (CNAME) of the initial domain name.</td>
</tr>
<tr>
<td><a href="https://US-support.acme.com">https://US-support.acme.com</a></td>
<td>A secondary custom URL that associates to a service portal on your instance. Your instance can support multiple custom URLs to the same service portal.</td>
</tr>
</tbody>
</table>

**Custom URL considerations outside of your instance**

Before you can associate a custom URL, you must own (or purchase) a URL through a domain provider. There are also specific configurations necessary before you can create and associate a custom URL on your instance.

**Custom URL configurations**

<table>
<thead>
<tr>
<th>Configuration items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the CNAME with the provider</td>
<td>The CNAME record must be set as the ServiceNow instance URL.</td>
</tr>
</tbody>
</table>
### Configuration items

<table>
<thead>
<tr>
<th>Configuration items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determine your dedicated VIP status</td>
<td>Your ServiceNow instance must be on a dedicated Virtual IP (VIP) address. Most are. To confirm if your instance uses a VIP, contact Customer Service and Support.</td>
</tr>
</tbody>
</table>

**Note:** When deleting or updating CNAME records which point to your instance, you must follow this sequence to avoid dangling records in the instance. First, delete the CNAME records from your instance and then remove or update the CNAME setting at your DNS provider.

### Activate custom URLs

Enable custom URLs to be set up on your ServiceNow instance. You can activate the Custom URL plugin (com.snc.customurl) if you have the admin role.

Role required: admin

1. Navigate to **System Definition > Plugins**.
2. Find and click the **Custom URL** plugin.
   
   **Note:** Do not select the **Custom URL - Internal** plugin, which is an internal component for scripted custom URL APIs.

3. On the Custom URL record, click the **Activate/Repair** related link.
4. In the Plugin Activation window, click **Activate**.
   
   When the Plugin Activation window reopens with a message that the plugin is activated, click **Close & Reload Form** to stay on this form.

5. In the Plugin Files related list, find the following property, and change the setting value:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.customurl.enabled</td>
<td>To enable custom URLs, set the value to <strong>True</strong>. By default, this property is set to <strong>False</strong>, which means that you cannot associate a custom URL.</td>
</tr>
</tbody>
</table>
   
   **Note:** To disable this feature, set this property back to **False**.

6. Click **Update**.

### Set a custom URL as the instance URL

Add a custom URL to your instance configuration to use instead of your ServiceNow URL.

Role required: admin

You must activate the custom URL plugin and have purchased or registered a URL before adding the custom URL to your instance.

1. Navigate to **Custom URL > Custom URLs**. You should either:
   
   - Click **New** to associate a new domain name that is new to your instance.
   - Select a custom URL already set up to set as your instance URL.
2. Fill in the appropriate fields:

### Custom URL fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name</td>
<td>Fully qualified domain name (FQDN) of the custom URL. The FQDN is a CNAME redirect created in the name server record for the custom domain.</td>
</tr>
<tr>
<td>Is Instance URL</td>
<td>Check box to enable this custom URL for all outbound URLs. Only one active custom URL can be the instance URL. To enable this setting for a custom URL, click Set as Instance URL on the URL record. Any previous custom URLs are then removed.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the custom URL record. If the status is Active, the custom URL is provisioned and ready to use.</td>
</tr>
<tr>
<td>Service Portal</td>
<td>Service portal that you want to use when you redirect users to your instance using the custom URL.</td>
</tr>
</tbody>
</table>

A custom URL should activate within six hours on your instance. A background job polls for custom URL job completion every 30 minutes.

### Custom URL datacenter job information

Every custom URL that is associated to your instance has a corresponding ServiceNow datacenter job which runs and shows URL information that is pertinent to your instance as described in the table.

<table>
<thead>
<tr>
<th>Job field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job ID</td>
<td>Unique ID of the job that checks the domain of the custom URL.</td>
</tr>
<tr>
<td>Last Run At</td>
<td>Date and time when the job last ran.</td>
</tr>
<tr>
<td>Payload</td>
<td>List of domains or custom URLs that were sent to the datacenter for CERT provisioning.</td>
</tr>
<tr>
<td>Poll Count</td>
<td>Number of times that the results have polled for this job.</td>
</tr>
<tr>
<td>Result</td>
<td>Verifies and validates each domain or custom URL sent in a payload.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the datacenter job.</td>
</tr>
</tbody>
</table>

### Generate SP metadata for SAML/SSO custom URL installations

A SAML or SSO installation needs the SP metadata generated for the IdP before the custom URL instance generates.
Role required: admin

The IdP needs SP metadata for the instance to authenticate and forward requests.

**Note:** Adding the Assertion Consumer Service URL (SP login URL) might be different for each IdP (Azure, ADFS, or Okta).

1. Choose your installed SSO plugin:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-Provider SSO</td>
<td>Navigate to Multi-Provider SSO &gt; Identity Providers. Choose an IdP and click the Generate Metadata button. The integration automatically generates the instance's SP metadata from the system property settings.</td>
</tr>
<tr>
<td>SAML 2 SSO</td>
<td>Navigate to SAML 2 Single Sign-on &gt; Metadata. The integration automatically generates the instance's SP metadata from the system property settings.</td>
</tr>
</tbody>
</table>

2. Copy the SP metadata in the text box.

For example:

```xml
<entityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://yourinstance.service-now.com">
  <SPSSODescriptor AuthnRequestsSigned="false"
    WantAssertionsSigned="true"
    protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <SingleLogoutService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
      Location="https://yourinstance.service-now.com/navpage.do" />
    <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
    <AssertionConsumerService isDefault="true" index="0"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="https://yourinstance.service-now.com/navpage.do" />
    <AssertionConsumerService index="1"
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="https://yourinstance.service-now.com/consumer.do"/>
  </SPSSODescriptor>
</entityDescriptor>
```

3. Provide the instance SP metadata to the IdP.

For example, SSOCircle allows a user to provide the SP metadata online.

4. Optional: To set up custom URLs in Azure:
   a) Go to **App Registrations**
   b) Select **All apps** from the dropdown menu
   c) Select the **ServiceNow App** and click settings

5. Optional: To use OAuth authentication, set up the redirect URL as all the registered custom URLs in the OAuth application endpoint configuration for the external client applications.

The redirect URL is synonymous with the callback URL that the authorization server redirects to.

6. Optional: To use Google reCAPTCHA service, set up an API key pair.
Custom URL errors and fixes

A list of common errors and associated fixes for a custom URL setup and configuration.

## Errors during setup

<table>
<thead>
<tr>
<th>Error message</th>
<th>Fix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unable to create a Custom URL. Try again later.</td>
<td>There might be an issue outside of your control interfering with the custom URL creation. Run at a different time before contacting support.</td>
</tr>
<tr>
<td>Unable to submit your new Custom URL request because another Custom URL request for your instance is still in progress.</td>
<td>Check the status on your Custom URL Jobs before you submit a new request.</td>
</tr>
<tr>
<td>You must clear the following properties before the instance URL can be set: Glide Proxy, Glide Servlet.</td>
<td></td>
</tr>
<tr>
<td>The provisioning of <code>&lt;custom_domain&gt;</code> is still in progress. This process can take up to X hours. Your instance administrator will receive a notification when this process completes.</td>
<td>After the provisioning on an instance starts for a custom URL, you must wait for the process to complete before the status changes.</td>
</tr>
<tr>
<td><code>&lt;custom_domain&gt;</code> is now set as the new instance URL. <code>&lt;base.service-now.com&gt;</code> is still in service, but all new URLs, such as in notifications, will use <code>&lt;custom_domain&gt;</code>.</td>
<td>Only one URL can be designated as the instance URL. The other URLs that are associated with your instance can be active, but only the instance URL can use notifications.</td>
</tr>
<tr>
<td>The Custom URL <code>&lt;custom_domain&gt;</code> is set to be immediately removed from the instance configuration and revert back to <code>&lt;base.service-now.com&gt;</code>. <code>&lt;custom_domain&gt;</code> continues an association to this instance as long as the CNAME record in your DNS is set.</td>
<td>This message confirms that you intend to change your custom URL. By accepting this confirmation, you initiate the change of the URL to your instance. Any URL that is on your Domain Name list, as a custom URL, can be active unless you remove it from the CNAME record on your provider.</td>
</tr>
<tr>
<td>You cannot modify glide.servlet.uri. This property is set by Custom URL.</td>
<td></td>
</tr>
<tr>
<td>You cannot modify glide.proxy.host. This property is set by Custom URL.</td>
<td></td>
</tr>
<tr>
<td>The CNAME record for <code>&lt;custom_domain&gt;</code> does not point to <code>&lt;base.service-now.com&gt;</code>.</td>
<td>The configuration on the URL provider side is not correct. Check your configuration on the CNAME record.</td>
</tr>
<tr>
<td>Missing CNAME record for <code>&lt;custom_domain&gt;</code>.</td>
<td>The CNAME record must be configured from your URL provider before the custom URL can be set for your instance.</td>
</tr>
</tbody>
</table>

**Note:** It usually takes 30 minutes to create a custom URL. If it is taking longer, contact https://support.servicenow.com/now?draw=case.
Enable password policies on your instance

Implement password policy controls at login to force users to change their password if the password does not meet the password policy criteria.

Role required: admin

The Password Policy [com.glide.password_policy] plugin is enabled by default. It goes into effect when a user changes or resets their password. If you customized your instance, via the ValidatePasswordStronger installation exit or your Password Reset credential store [pwd_cred_store], see password policy properties.

1. Navigate to Password Policy > Password Policies.
2. Click the available password strength preset that is initially set as Default.
   
   The password strength preset is the password policy that you apply to your instance. You can leave default as your instance password policy or you can select other options as described in the next step.

3. To customize your password policy, choose the password strength preset that applies to your organization:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Default password policy that is applied to your instance.</td>
</tr>
<tr>
<td>Medium</td>
<td>Password policy preset that minimizes the minimum character options to apply to your password policy criteria.</td>
</tr>
<tr>
<td>High</td>
<td>Password policy preset that increases some of the minimum character options to apply your password policy criteria.</td>
</tr>
<tr>
<td>Custom</td>
<td>Password policy preset that enables you to edit all of your password policy criteria.</td>
</tr>
</tbody>
</table>

4. On the form, fill in the fields.

   **Password Policy form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Password Length</td>
<td>Minimum length of the password. The password cannot have fewer than 8 characters.</td>
</tr>
<tr>
<td>Maximum Password Length</td>
<td>Maximum length of the password. The default is 40 characters.</td>
</tr>
<tr>
<td>Minimum Uppercase Character(s)</td>
<td>Minimum number of uppercase characters in the password, from 0 to 10.</td>
</tr>
<tr>
<td>Minimum Lowercase Character(s)</td>
<td>Minimum lowercase characters in the password, from 0 to 10.</td>
</tr>
<tr>
<td>Minimum Numeric Character(s)</td>
<td>Minimum numeric of characters in the password, from 0 to 10.</td>
</tr>
<tr>
<td>Minimum Special Character(s)</td>
<td>Minimum number of special characters in the password, from 0 to 10.</td>
</tr>
<tr>
<td>Include Special Characters</td>
<td>Restricted set of characters. If you must allow a restricted set of special characters, delimit the restricted set by commas. For example, if you enter &quot;$,!” users can only use &quot;$&quot; and &quot;!” as special characters in their password. No other special characters can be used, and a password with other special characters is not allowable.</td>
</tr>
</tbody>
</table>

5. Optional: To test that a password meets the policy criteria, enter a password and click Test Your Password.
   
   The password comes back as valid or invalid. If a password is invalid, error messages display the criteria rules that are not met.
6. Click **Update**.

**Password policy properties**

The password policy properties enable you to administrate password policies, exclude list passwords, and apply a password policy upon login.

Go to **System Property > All Properties** to view and edit the password policy properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.enable.password_policy</td>
<td>This property enables a password policy for your instance which goes into effect when a user changes their password or resets their password. The default is true.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If your instance has been customized, via the ValidatePasswordStronger installation exit or your Password Reset credential store [pwd_cred_store], you must create this property and add to your system properties.</td>
</tr>
<tr>
<td>glide.enable.blacklist_password</td>
<td>This property prohibits using specific passwords. The administrator can insert passwords into the Excluded Password table. The default is true.</td>
</tr>
<tr>
<td>glide.apply.password_policy.on_login</td>
<td>This property forces users to change their passwords during their next login, if their existing passwords are not in compliance with the current password policy. The default is false. Setting the value to true enforces a password policy upon login.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Enabling this property might force a significant number of users to change passwords that are not in compliance with a new password policy.</td>
</tr>
</tbody>
</table>

**Exclude passwords through password policies on your instance**

You can add passwords to the Excluded Password table to prohibit specific passwords from being used by users on your instance.

Role required: admin

1. Navigate to **Password Policy > Excluded Passwords**.
2. Click **New** and enter the password to add to your exclude list.

You can add as many passwords to your list as necessary.

**Enable external users to self-register to your ServiceNow instance**

Use external user self-registration to on-board a large volume of external users to your instance. This feature enhances identity verification to improve customer experiences and supports commonly used registration flows.

External user self-registration enables a large group of users to register to a ServiceNow app without the help of an administrator. For example, a university with a large group of students needing on-campus parking could register...
themselves to the campus parking app. Each student would be given a limited set of privileges specific to parking, and would complete an automated registration process. This system could generate a parking number, unique to each student, and insure they had a parking space.

A self-registration flow consists of a custom ServiceNow app, in this case, a campus parking app. After configuring an app with necessary tables, an administrator would configure the registration, including a pre-registration flow, field mapping, post registration mapping, captcha, role mapping and post registration flow.

**Activate External User Self-Registration**

You can activate the External User Registration plugin (com.snc.external_user_self_registration) if you have the admin role.

Role required: admin

1. Navigate to **System Applications > All Available Applications > All.**
2. Find the plugin using the filter criteria and search bar.
   - You can search for the plugin by its name or ID. If you cannot find a plugin, you might have to request it from ServiceNow personnel. For more information, see Request a plugin.
3. Click **Install**, and then in the Activate Plugin dialog box, click **Activate**.

**Note:** When domain separation and delegated admin are enabled in an instance, the administrative user must be in the global domain. Otherwise, the following error appears: Application installation is unavailable because another operation is running: Plugin Activation for <plugin name>.

**External roles in self-registration**

To prevent inadvertently providing access to external users, you can assign the snc_external role to all external users.

External users that self-register must be assigned the snc_external role, which has the least privileges. The snc_external role indicates that the user is external to your organization and should not have any access to resources unless explicitly allowed through ACLs for the snc_external role or additional roles that inherit the snc_external role.

By default, users with the snc_external role cannot access:

- Scripted REST API resources that are not marked external.
- Tables without the role that inherits the snc_external role or the public role.
- Non-record type resources, such as processors and UI pages without the snc_external role or a role that inherits the snc_external role.
- Now Intelligence dashboards.

Beginning with the Paris release, you must enable an exclude-list property to enforce the explicit assignment of snc_external roles. For information about enabling the property, see Prevent future internal role assignments for external users.

**Create a user registration configuration for external users**

Create a user registration configuration record to bootstrap the onboarding process of external users to custom ServiceNow applications. This form guides the external users through the self-registration process.

- Role required: admin
- Activate External User Self-Registration

1. Navigate to **External User Self-Registration > User Registration Configurations** and click **New**.
2. On the form, fill in the fields.
## User registration configuration form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the registration form. For example, a student parking registration might be Parking Management Students.</td>
</tr>
<tr>
<td>Roles assigned to provisioned users</td>
<td>Roles assigned to the provisioned users. The specified roles have to extend or contain the <code>snc_external</code> role. The specified role can also be <code>snc_external</code> role. For external users, each role must have an <code>snc_external</code> to note an external user. If you have pre-configured roles, the roles should be accessible when you unlock the roles and search for users.</td>
</tr>
<tr>
<td>Enable terms and conditions</td>
<td>Option to add a terms and conditions URL to the registration page.</td>
</tr>
<tr>
<td>Terms and conditions URL</td>
<td>The publicly accessible URL which contains the terms and conditions of the registration form. This field appears only when Enable terms and conditions is selected.</td>
</tr>
<tr>
<td>Description</td>
<td>The description of the registration form. This field appears only when you save or submit the configuration. You can add more information about the registration form in this field.</td>
</tr>
<tr>
<td>Note:</td>
<td>You can only add a description after you save or update a user registration configuration.</td>
</tr>
<tr>
<td>Application</td>
<td>Application containing this record. The application is automatically set to Global.</td>
</tr>
<tr>
<td>Active</td>
<td>Option which makes the user registration configuration active. This option is selected by default.</td>
</tr>
<tr>
<td>Enable CAPTCHA</td>
<td>Option to add a CAPTCHA to the registration form. The default CAPTCHA provider is Google reCAPTCHA.</td>
</tr>
<tr>
<td>Note:</td>
<td>To enable CAPTCHA for user registration, follow the steps in Configure Google reCAPTCHA for external user self-registration.</td>
</tr>
</tbody>
</table>
3. **Click Submit.**

A user registration configuration with the default settings is created.

<table>
<thead>
<tr>
<th>Name</th>
<th>Parking Management Students</th>
<th>Application</th>
<th>Global</th>
</tr>
</thead>
<tbody>
<tr>
<td>Roles assigned to provisioned users</td>
<td>snc_external</td>
<td>Active</td>
<td>✓</td>
</tr>
<tr>
<td>Enable CAPTCHA</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Terms and condition URL</td>
<td>example.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Parking Management for Students</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4. Optional: Configure the **Registration** tab to show fields and the order that they appear:

### Registration Form Fields

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display in Registration Form</td>
<td>Set any field you want to display as True.</td>
</tr>
<tr>
<td>Order</td>
<td>Set an order number to display fields on your form.</td>
</tr>
<tr>
<td>Mandatory</td>
<td>Set any field you want to make it mandatory as True.</td>
</tr>
<tr>
<td>Validation only field</td>
<td>Set any field you want to use only for validation. For example, registration code.</td>
</tr>
</tbody>
</table>

You can choose to display the default form fields or you can add custom form fields to the Registration Form. For more information, see **Default registration form fields**.

---

**Registration tab**

You can also add custom registration form fields. For more information, see **Add a custom registration form field**.
5. Optional: Configure the **Verification** tab to verify the identity of the registered users. When the user verification flow triggers, an activation link is sent to the user’s registered email address.

**Verification tab fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requires user verification</td>
<td>Option to trigger a user verification subflow which runs after user registration. The subflow is for user identity verification.</td>
</tr>
</tbody>
</table>
| User verification flow               | The subflow used to verify the identity of the user. The subflow triggers only when you enable user verification.  

The **External User Verification** subflow is available by default. You can create a copy of the default subflow in Flow Designer and modify it according to your requirements. For more information, see [Flow Designer](#).  

**Note:** To preview the **External User Verification** subflow in a new tab use the following shortcuts:  
- Macintosh: Command + Click  
- Windows: Control + Click

| Activation link expiry time (in hours) | The number of hours after which an activation link expires. The default value is 24. |

6. Optional: Configure the **Transformation** tab to map self-registered users and activated users.  

There are two transformation maps (u_reg_xmap_[number]) which automatically map the registered users from the User Acti Req [number] table to the Self Registered User [number] table. You can create a copy of these
default transformation maps and modify the map according to your requirements. For more information, see Transform maps.

<table>
<thead>
<tr>
<th>Transformation Maps</th>
<th>SourceTable</th>
<th>TargetTable</th>
<th>Run Business Rules</th>
<th>RowA</th>
<th>RowB</th>
<th>Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Registration</td>
<td>User Add Req 801776 [s_user_add_reg_801776]</td>
<td>User [sys_user]</td>
<td>true</td>
<td>100</td>
<td>true</td>
<td>2020-08-20 03:21:43</td>
</tr>
<tr>
<td>User Registration</td>
<td>User Add Req 801776 [s_user_add_reg_801776]</td>
<td>Self Reg User Profile 801776 [s_self_reg_user_profile_801776]</td>
<td>true</td>
<td>100</td>
<td>true</td>
<td>2020-08-20 03:21:44</td>
</tr>
</tbody>
</table>

Transformation tab
7. Configure the **Onboarding** tab to trigger subflows for onboarding activated users.

The default **External User Onboarding** subflow sends an email to the user that contains a link to reset their password. You can create a copy of the default subflow and modify it according to your requirements.

**Note:** When the **External User Onboarding** subflow triggers, the subflow sends an email to the user that contains a link to reset the password.

<table>
<thead>
<tr>
<th>Registration</th>
<th>Verification</th>
<th>Transformation</th>
<th>Onboarding</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Flow triggered after user account creation</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✗ User onboarding flow</td>
<td>External User Onboarding</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Onboarding tab
8. Optional: Configure the **Advanced** tab to map user tables and redirection pages of the registration form.
## Advanced tab

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration table</td>
<td>Name of the table where registration form information is saved.</td>
</tr>
<tr>
<td>Registration form field configuration</td>
<td>The record associated to the registration form in the Record Producer.</td>
</tr>
<tr>
<td>Activation table</td>
<td>Label and name of the table used for user activation. The activation table contains records of the users who have completed verification.</td>
</tr>
<tr>
<td>User table</td>
<td>Label and name of the user profile table.</td>
</tr>
<tr>
<td>Activation success page</td>
<td>The page to which a user redirects after the activation is successful.</td>
</tr>
<tr>
<td>Activation error page</td>
<td>The page to which a user redirects when the activation fails.</td>
</tr>
<tr>
<td>Post registration redirect page</td>
<td>The page to which user is redirected after registration.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Registration link label</td>
<td>The button name used for registration from the service portal. The default value is Register.</td>
</tr>
</tbody>
</table>

While making changes or after completing all changes in the user registration configuration, you can use the **Preview Registration Form** button to preview changes in the registration form.
# Parking Management Students

**Parking Management for Students**

- **First name**
- **Last name**
- **Email**
- **I agree to the Privacy Policy and Terms and Conditions**

**Sign Up**

**Required Information**

---

**Registration Form Preview**
Configure Google reCAPTCHA for external user self-registration

To use the Google reCAPTCHA service, you must request an API key pair from Google and then configure the related system properties.

- Request an API key pair (a site key and a secret) from Google at https://www.google.com/recaptcha.
- Role required: admin

1. Navigate to System Properties > All Properties.
2. Search for the following properties and set the values:

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.user.registration.google.recaptcha.secret</td>
<td>The secret authorizes communication between the application and the reCAPTCHA server. Type: password2</td>
</tr>
<tr>
<td>glide.user.registration.google.recaptcha.site_key</td>
<td>The site key is used to invoke reCAPTCHA service on your registration page. Type: string</td>
</tr>
</tbody>
</table>

Default registration form fields

You can use the default registration form fields or create custom registration form fields.

Registration form fields

The following form fields are added in the Registration form by default.

<table>
<thead>
<tr>
<th>Field Label</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Phone</td>
<td>Single line text</td>
</tr>
<tr>
<td>City</td>
<td>Single line text</td>
</tr>
<tr>
<td>Country</td>
<td>Select Box</td>
</tr>
<tr>
<td>EDU Status</td>
<td>Select Box</td>
</tr>
<tr>
<td>Email</td>
<td>Email</td>
</tr>
<tr>
<td>First name</td>
<td>Single line text</td>
</tr>
<tr>
<td>Gender</td>
<td>Single line text</td>
</tr>
<tr>
<td>Home phone</td>
<td>Single line text</td>
</tr>
<tr>
<td>Language</td>
<td>Select Box</td>
</tr>
<tr>
<td>Last name</td>
<td>Single line text</td>
</tr>
<tr>
<td>Middle name</td>
<td>Single line text</td>
</tr>
</tbody>
</table>

Note: This field is useful when the registration form is for an educational institution.
<table>
<thead>
<tr>
<th>Field Label</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile phone</td>
<td>Single line text</td>
</tr>
<tr>
<td>Name</td>
<td>Single line text</td>
</tr>
<tr>
<td>Prefix</td>
<td>Select Box</td>
</tr>
<tr>
<td>Title of the user. For example, Mr., Dr., and so on.</td>
<td>Select Box</td>
</tr>
<tr>
<td>State / Province</td>
<td>Single line text</td>
</tr>
<tr>
<td>Street</td>
<td>Wide Single Line Text</td>
</tr>
<tr>
<td>Title - Job title</td>
<td>Select Box</td>
</tr>
<tr>
<td>Zip / Postal code</td>
<td>Single line text</td>
</tr>
</tbody>
</table>

**Note:** You cannot delete the default registration form fields.

**Add a custom registration form field**
You can add custom fields in the user self-registration form.

Role required: admin

1. Navigate to **External User Self-Registration > User Registration Configurations**.
2. Open the record for the required user registration configuration.
3. Navigate to the end of the Registration Form Fields section and click **Insert a new row**.
4. Enter the field name under the **Label** column and click check mark.

A new row is added with the default values. You can configure the custom registration form field based on your requirements.

**Registration Form Field Columns**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>The field name which appears on the registration form.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of the user interface element. Following are the supported types:</td>
</tr>
<tr>
<td></td>
<td>- Single line text</td>
</tr>
<tr>
<td></td>
<td>- Email</td>
</tr>
<tr>
<td></td>
<td>- Date</td>
</tr>
<tr>
<td></td>
<td>- Date/time</td>
</tr>
<tr>
<td></td>
<td>- Yes/No</td>
</tr>
<tr>
<td></td>
<td>- Wide Single Line Text</td>
</tr>
<tr>
<td></td>
<td>- Multiple Choice</td>
</tr>
<tr>
<td></td>
<td>- Select Box</td>
</tr>
<tr>
<td>Display in Registration Form</td>
<td>Option to display the field in the registration form.</td>
</tr>
<tr>
<td>Order</td>
<td>The sequence in which the form fields appear on the registration form.</td>
</tr>
<tr>
<td></td>
<td>The field with the lowest order value appears first and the field with the highest order value appears last. The default value is 10,000.</td>
</tr>
<tr>
<td>Mandatory</td>
<td>Option to make a field mandatory on the registration form.</td>
</tr>
</tbody>
</table>
### Validation only field

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validation only field</td>
<td>Option to use a field only for validation purposes. For example, registration code. When set to true, this field is not saved in the User Table (sys_user).</td>
</tr>
</tbody>
</table>

5. Save or Update the changes.

---

**Enable external user self-registration for Service Portal**

Enable external users to register to an app through Service Portal.

Role required: admin

1. Navigate to **Service Portal > Portals**.
2. Open a portal record.
3. On the form, fill in the **External user registration configuration** field.
   - Select a user registration configuration.
4. Click **Update**.

The login widget includes a link to the registration form that you previously configured.
Verify user self-registration requests

After a user registers from the Service Portal, a user record is added to the Registration Requests module. You can view the list of registered users who have successfully registered in the Service Portal.

Role required: admin

1. Navigate to **External User Self-Registration > Registration Requests**.
   The list of user records are displayed.

2. (Optional) Review the individual user records and modify according to your requirements. For example, you can change the status of a user record form **Pending** to **Processed**.
Normalization Data Services

The Normalization Data Services plugin helps maintain consistency for table fields that refer to a company name. Tables related to configuration items and assets usually contain columns referring to a company name, such as a vendor or manufacturer. Often, these tables refer to the same company by several different names. This situation can happen for many reasons. For example, vendors sometimes use different company names depending on the device. This inconsistency creates problems, especially for reports that rely on these company names.

The Normalization Data Services plugin helps alleviate this problem.

When you enable and configure the Normalization Data Services plugin, the system downloads a list of standard company names that ServiceNow has compiled. It also downloads a list of common variants of that name. Any time the plugin finds a company-name field with one of those variants, it substitutes the standard name in its place.

**Note:** The Normalization Data Services plugin refers to a standard name as a normalized name and to a variant name as a discovered name.

While the Normalization Data Services plugin provides services similar to the field normalization feature, this plugin does not require you to manually set up the mappings from one name to another. If you like, you can add your own mappings to the set. However, you automatically start with extensive lists of common company names (normalized names) and their variants (discovered names).

The Normalization Data Services plugin stores data in two tables. The Normalized Company Names table contains the list of normalized company names. The Normalized Mappings table contains the mappings between each discovered name and its normalized name.

**CAUTION:** If you edit a field whose value is a normalized name, you change the normalized name for ALL discovered names that map to it. These types of updates occur regardless of the table in which you edit the field.

Using guided setup to implement Normalization Data Services

Normalization Data Services guided setup provides a sequence of tasks that help you configure the Normalization Data Services plugin on your ServiceNow instance. To open Normalization Data Services guided setup, navigate to Normalization Data Services > Guided Setup. For more information about using the guided setup interface, see Using guided setup.

**Note:** Because the Normalization Data Services feature requires an internet connection to download mapping information, this feature is not supported for on-premise instances.

Normalized Company Names table

The Normalization Data Services plugin stores the normalized company names in the Normalized Company Names table.

**Normalized company names fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The normalized name for this company.</td>
</tr>
<tr>
<td>Table</td>
<td>The table in which this name is stored.</td>
</tr>
<tr>
<td>Description</td>
<td>[optional] A description with further information about this company or record.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
<td>The field in which this name is stored.</td>
</tr>
<tr>
<td>Customer override</td>
<td>True, if the customer has an override in place for this name. Otherwise, false.</td>
</tr>
</tbody>
</table>

### Normalized company names related lists

<table>
<thead>
<tr>
<th>List</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normalized mappings</td>
<td>A list of all the discovered names that map to this normalized name.</td>
</tr>
</tbody>
</table>

### Normalized Mappings table

The Normalized Mappings table lists all the discovered names and the normalized name to which each maps.

#### Normalized mappings fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovered name</td>
<td>A variant of a normalized name in the database.</td>
</tr>
<tr>
<td>Normalized name</td>
<td>The normalized name to which the discovered name maps.</td>
</tr>
<tr>
<td>Table</td>
<td>The table in which this name is stored.</td>
</tr>
<tr>
<td>Field</td>
<td>The field in which this name is stored.</td>
</tr>
</tbody>
</table>

### Normalized company names related lists

<table>
<thead>
<tr>
<th>List</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Related mappings</td>
<td>A list of all the discovered names that map to the same normalized name as the selected record.</td>
</tr>
</tbody>
</table>

### Actions

<table>
<thead>
<tr>
<th>List</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Promote discovered name</td>
<td>Replaces the normalized name with the discovered name for the selected record and for all the records in its related mappings list.</td>
</tr>
</tbody>
</table>
Normalization Properties

On the Normalization Properties form, you can see and change the configurable properties for the Normalization Data Services plugin.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reference qualifiers on all tables that reference Company will be updated to use the Normalized field.</td>
<td>If Yes, any reference field for Company – for any table across the platform – uses the Normalized name. This service only works if you have run the Update Reference Qualifiers task in the Guided Setup.</td>
</tr>
<tr>
<td>Enable business rule that automatically normalizes manufacturer names for configuration items.</td>
<td>If Yes, the system normalizes company names when you add or update configuration items by a mechanism other than Discovery (such as by manual import sets).</td>
</tr>
<tr>
<td>Enable Discovery to use the normalization service for manufacturer name.</td>
<td>To have Discovery use the normalized company name for the manufacturer name, click Yes.</td>
</tr>
<tr>
<td>This property is to enable or disable the Normalization API.</td>
<td>To enable the Normalization Data Service API, click Yes. To disable, click No. For details, see Normalization Data Services.</td>
</tr>
</tbody>
</table>

Changing normalized company names

You can change a normalized company name several different ways. In all cases, that change affects all normalized fields referring to that company.

You have several options for changing a normalized company name:

• Edit the Normalized Name field in the Normalized Mappings table. This method is preferred.
• Edit the Normalized Company name table.
• Edit the Company Name field on any table that refers to the Company [core_company] table.

CAUTION: If you edit a field whose value is a normalized name, you change the normalized name for ALL discovered names that map to it.

Change a normalized company name

You can change normalized company names by editing records in the Normalized Company Name table.

Role required: admin

You can edit records in the Normalized Company Names tables, but you cannot add records to it.

1. Navigate to User Administration > Normalization Data Services > Normalized Mappings.
2. Find the record with the name you want to replace and edit the Normalized name field.

The system changes the Normalized Company name for every discovered name that maps to that normalized name.
Metrics

A metric measures and evaluates the effectiveness of IT service management processes.

For example, a metric could measure the effectiveness of the incident resolution process by calculating how long it takes to resolve an incident.

A metric can often be easily obtained from the data. To find the number of incidents created today, a report counts the number of incidents in the incident table with a Created date of today. However, metrics must be gathered as data is updated. For example, determining how long an incident was assigned to a certain group requires collecting information about assignment changes and calculating the duration of each assignment.

The Metric plugin provides an easy, declarative way of defining metrics. Once defined, the data for the metric is gathered, and instances of the metric are calculated and stored. For example, the "Assigned to Duration" metric measures the amount of time an incident is assigned to an individual. To define this metric, you create a metric definition of the type "Field value duration" and select the "Assigned to" field from the Incident table. A metric instance is created for each incident assignment showing its duration. Reporting on the duration of incident assignments becomes easy.

You can report on a metric by using a database view that links the metric to the table on which it is defined.

To install the Metric Definition plugin (com.glide.metrics), navigate to System Definition > Plugins, search for Metric Definition, and click Install.

Create a metric

Create a metric definition for a task table.

Role required: metric_admin

1. Navigate to Metrics > Definitions.
2. Click New.
3. Complete the Metric definition form then click Submit.

New metric definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>The system generates a unique record number for the metric definition.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter a unique name to describe what metrics are collected.</td>
</tr>
</tbody>
</table>
| Table | Select the table that you want to collect metrics for. A metric can only apply to one table.  
**Note:** The list shows only tables and database views that are in the same scope as the metric definition |
| Field | Select the table column you want to monitor for changes. Metrics only work on audited fields. Creating a metric for non-audited field produces unreliable metrics.  
**Note:** Fields starting with 'sys_' will not work for a metric definition, with the exception of 'sys_domain'. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select what values this metric generates.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Field value duration</strong>: This type of metric measures the duration of</td>
</tr>
<tr>
<td></td>
<td>time from when the value of the specified field is set until it is</td>
</tr>
<tr>
<td></td>
<td>changed. A Field value duration metric can optionally specify a script.</td>
</tr>
<tr>
<td></td>
<td>The script can either return a duration value or set the answer variable</td>
</tr>
<tr>
<td></td>
<td>to false to stop processing the metric. For example, the baseline</td>
</tr>
<tr>
<td></td>
<td>incident metrics stop calculating duration when the Active field of an</td>
</tr>
<tr>
<td></td>
<td>incident is set to false. The script can also carry out any other action</td>
</tr>
<tr>
<td></td>
<td>such as closing the duration of other metrics defined on the same record.</td>
</tr>
<tr>
<td></td>
<td>See the example script for more information.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Script calculation</strong>: This type of metric creates a metric instance</td>
</tr>
<tr>
<td></td>
<td>using a script. The script has access to the current row in the table</td>
</tr>
<tr>
<td></td>
<td>(for example an incident) and the metric definition. The script must</td>
</tr>
<tr>
<td></td>
<td>perform metric calculations and insert data into the metric_instance table.</td>
</tr>
<tr>
<td></td>
<td>The calculation does not have to result in a duration. It can calculate</td>
</tr>
<tr>
<td></td>
<td>any type of value and store it in the metric instance value.</td>
</tr>
<tr>
<td>Timeline</td>
<td>Check this box to display the metric on a Timeline pages.</td>
</tr>
<tr>
<td>Active</td>
<td>Check this box to monitor changes for this metric.</td>
</tr>
<tr>
<td>Description</td>
<td>[Optional] Specify what data the metric monitors and it's conditions.</td>
</tr>
<tr>
<td>Script</td>
<td>Enter the script you want the metric to run to either calculate a duration</td>
</tr>
<tr>
<td></td>
<td>or perform some calculation on the metric_instance table.</td>
</tr>
</tbody>
</table>

**Note:** In the base system, metrics are configured to work on the task table only. To apply metrics to cmdb_ci tables, duplicate the metric events business rule that currently runs on the task table for the cmdb_ci table. Without the events created, no metric processing can occur.

**Sample field value duration script**

Review the existing Incident Open metric definition to see how you can create your own custom metric.

This script either provides a duration value or stops processing durations (sets the answer variable to `false`) when an incident is closed.

```java
// script can set answer to false to terminate processing of the metric
// mi - MetricInstance
// answer
if (!current.active) {
    answer = false;
    mi.endDuration();
    gs.log("Closing field durations");
    closeDurations(mi.current);
}
```
function closeDurations(current) {
    var now_GR = new GlideRecord('metric_instance');
    gr.addQuery('id', current.sys_id);
    gr.addQuery('calculation_complete', false);
    gr.addQuery('definition.type', 'field_value_duration');
    gr.query();
    while (gr.next()) {
        gs.log("closing: " + gr.definition.name + " for: " + current.number);
        var definition = new GlideRecord('metric_definition');
        definition.get(gr.definition);
        var mi = new MetricInstance(definition, current);
        mi.endDuration();
    }
}

**Metric instance**

A metric instance is a record in the metric_instance table. A record holds one instance of a metric.

Metric instance records get created and updated in one of two ways: 1) If the metric is a duration, the system automatically populates the metric instance table with duration values. 2) If the metric is calculated from a script, the script itself must populate the metric_instance table.
Some of the notable fields in the metric_instance table are:

- **Metric definition**: the metric definition for which this metric instance was gathered.
- **Value**: For a "Field value duration" metric this is the value of the table field for which duration is calculated. For example, for the "Assigned to Duration" metric, the Value is the name of the person assigned to the incident. For other metrics, the value can be any value calculated by the metric.
- **ID**: Identifies the specific record for which the metric is gathered. For example, the specific incident.
• **Duration**: Time duration for a Field value duration metric.

## Platform performance

Ensure system optimization through performance monitoring and diagnostics.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application server response</td>
<td>Time for the application server to process a request and render the resultant page.</td>
</tr>
<tr>
<td>Network latency and throughput</td>
<td>Time for the network to pass your request to the server and the response back.</td>
</tr>
<tr>
<td>Browser rendering and parsing</td>
<td>Time for your browser to render the HTML and parse/execute Javascript.</td>
</tr>
<tr>
<td>Instance Cache</td>
<td>Amount of system resources available for processing.</td>
</tr>
</tbody>
</table>

## Instance cache effects on performance

There is a performance degradation whenever you purge and rebuild the instance cache. During core business hours, avoid or minimize any of the following actions that will cause a purge and rebuild of the instance cache.

- Adding or updating system properties
- Adding or updating dictionary entries
- Committing update sets
- Adding or updating translations

## Transaction log response times

The instance automatically logs the vital statistics of every transaction it processes, and that information is available to you as an administrator.

To look at the log, navigate to **System Logs > Transactions**.

To see the average response time of all listed transactions, right-click the column **Response time**. Select **Configure > List Calculations**, and then select the **Average value** check box.

It is a good practice to limit the list to those transactions that took place during the time period of interest. The default filter returns transactions from today.
Transaction log

For each completed transaction, the following information is available (times are in milliseconds):

- Date/time, User ID, IP address, and URL of the transaction.
- Total response time, which does not include the browser time because the server does not have that information.
- **Network time**: network transmission time, both from and to the user.
- **SQL time**: time spent executing SQL commands.
- **SQL count**: number of SQL commands executed.
- **Business rule time**: time spent processing business rules.
- **Business rule count**: number of business rules executed.
- **Output length**: how many bytes the transaction returned, after any compression.

Response time on forms

A response time indicator (clock) appears at the bottom right of many forms and lists.

This indicator provides the processing time for a completed transaction, including the total time and the time for each step. Click the icon to show and hide the response time details. Point to the icon to see a tooltip with the details. The following example shows the response time for retrieving a filtered list in a demo instance.

Response time

In this example, the transaction took the following amount of processing time:

- 1019 milliseconds total time
- 3 milliseconds moving data across the network
• 526 milliseconds on the server

**Note:** Server time is calculated using the following formula:

\[ \text{server time} = (\text{client response time} - \text{browser time} - \text{client network time}) \]

• 490 milliseconds in the browser, rendering the HTML and parsing and executing JavaScript

Response does not appear for simple operations, such as paging, changing a list sort order, or for the first transaction in a session.

To view a detailed breakdown of the browser processing time on forms, click **browser**.

Administrators can disable the response time by setting the `glide.ui.response_time` property to `false`.

When you review response times, look for the following issues.

1. A period where all transactions took an unusually long time. For example, transactions that normally took 1 second took 15 seconds between 11:00 AM and 11:20 AM. This issue can indicate that an unusual load, such as a large report, ran on that app server during that time.

2. A specific transaction which repeatedly took an unusually long time. For example, the list of closed incidents sorted by short description took 30 seconds each time it was displayed. This issue can indicate that a particular transaction put an unusual database load on the system, such as sorting 500,000 records on an unindexed field.

Try the following actions to improve performance.

1. Look for one or more transactions that span the entire window. For example, you observe that the response was slow for six minutes and one transaction ran the entire time. You can try adding additional indexing to the database to make the transaction faster. Certain types of queries are always going to run more slowly than others, regardless of indexing.

2. Ensure that a cache flush is not being run during business hours. Cache flushes are intended to prevent older data from interfering with changes and updates, and are performed automatically when using update sets. Scheduled cache flushes, using `cache.do`, can affect overall performance, and degrade system response times. Do not run cache flushes during business hours, and do not trigger cache flushes automatically.

3. If you cannot find any specific issues when experiencing slow response time, contact support to see if there are global issues with the application server hardware.
Client transaction timings

The Client Transaction Timings plugin provides extra information about the amount of time spent on both the client and server side, and by the browser and network. This feature not only helps find long-running processes, but also provides information about where in the process the performance issue is caused.

Network response times

Troubleshooting a poor network response time can be difficult, but there are certain quick tests you can perform.

One clear indicator of a network issue is when you find that users in one location have good performance, and users in another location have poor performance. That tells you that the server and application are fine. Assuming that browser settings are identical, the only meaningful difference is the network.

Ping times

The coarsest measure of network response time is a ping. A ping measures the total time for a packet to make it from the source machine to the target and back again.

To perform a ping in Windows, bring up a command window (DOS prompt) and type:

```bash
ping -t <yourinstancename>.service-now.com
```

```
Microsoft Windows [Version 6.0.6000]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.
C:\Users\Admin>ping -t www.service-now.com
Pinging www.service-now.com [70.85.100.85] with 32 bytes of data:
  Reply from 70.85.100.85: bytes=32 time=37ms TTL=55
  Reply from 70.85.100.85: bytes=32 time=36ms TTL=55
  Reply from 70.85.100.85: bytes=32 time=57ms TTL=55
  Reply from 70.85.100.85: bytes=32 time=44ms TTL=55
  Reply from 70.85.100.85: bytes=32 time=37ms TTL=55
  Reply from 70.85.100.85: bytes=32 time=36ms TTL=55
  Reply from 70.85.100.85: bytes=32 time=36ms TTL=55
  Reply from 70.85.100.85: bytes=32 time=85ms TTL=55
  Reply from 70.85.100.85: bytes=32 time=36ms TTL=55
  Reply from 70.85.100.85: bytes=32 time=39ms TTL=55
  Reply from 70.85.100.85: bytes=32 time=49ms TTL=55
  Reply from 70.85.100.85: bytes=32 time=39ms TTL=55
  Reply from 70.85.100.85: bytes=32 time=36ms TTL=55
  Reply from 70.85.100.85: bytes=32 time=41ms TTL=55

Ping statistics for 70.85.100.85:
  Packets: Sent = 14, Received = 14, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 36ms, Maximum = 85ms, Average = 43ms
```

Look for a time under 100 ms if you are in the U.S., or 150 ms if you are in Europe or Asia. In practice, anything less than 250 ms is not of concern as it is not generally a major component in your perceived response time.
Traceroute

If you are seeing slow ping times, you can run a traceroute. Some networks refuse to forward ICMP, and your traceroute request may not work. If it does work, it is a great tool for identifying network bottlenecks. To run a traceroute on Windows, bring up a command window and run the following command.

```
tracert <yourinstancename>.service-now.com
```

Sample output:

```
C:\dev\mysql5\bin>tracert mycompany.service-now.com
Tracing route to mycompany.service-now.com [70.87.98.130]
over a maximum of 30 hops:
1    1 ms    1 ms    1 ms  12.192.116.193
2    4 ms    4 ms    4 ms  12.116.227.37
3   32 ms   32 ms   32 ms  gbr1-p90.sd2ca.ip.att.net [12.123.145.178]
4   33 ms   33 ms   33 ms  tbr1-p013503.phmaz.ip.att.net [12.122.2.142]
5   34 ms   34 ms   34 ms  tbr2-cl1521.phmaz.ip.att.net [12.122.10.194]
6   32 ms   33 ms   33 ms  tbr2-cl1592.dllstx.ip.att.net [12.122.10.81]
7   31 ms   50 ms   31 ms  gar1-p370.dllrtx.ip.att.net [12.123.16.173]
8   31 ms   31 ms   31 ms  12.119.136.14
9   31 ms   31 ms   31 ms  te9-1.dsr02.dllstx3.theplanet.com [70.87.253.22]
10  37 ms   37 ms   37 ms  vl41.dsr01.dllstx4.theplanet.com [70.85.127.83]
11  31 ms   37 ms   31 ms  gi1-0-1.car16.dllstx4.theplanet.com [67.18.116.67]
12  32 ms   32 ms   32 ms  70.87.98.130
Trace complete.
```

Each line in the traceroute represents a network step between the source machine and the destination machine. In the sample traceroute, there were a total of 12 steps required to get the network traffic from the laptop to `<yourinstancename>.service-now.com`.

- The left column is the step number.
- The next three columns are latency estimates, performed three times to give an average.
- The last column is the machine you are hopping to.

For example, from rows #1 and #2 above, you can tell:

```
1    1 ms    1 ms    1 ms  12.192.116.193
2    4 ms    4 ms    4 ms  12.116.227.37
```

At the end of row 1, it was at 12.192.116.193. It then took 4 ms (on average) to get to 12.116.227.37.

Generally, with a traceroute, you are looking for individual steps that take a long time, like 500 ms for a particular hop. You are also looking for steps that show an asterisk (*) instead of a step time, for example:

```
1   100 ms  * 500ms  12.192.116.193
```

The asterisk indicates that a particular packet failed to arrive, which can indicate network problems on that particular hop. You also see an asterisk if that particular router is set to not forward ICMP. This outcome is potentially a false alarm if all three latency times for a step are asterisks.
Browser settings and performance

Depending on the browser you use, browser settings can affect the performance of your instance.

Web pages in your instance can be large, for example, over 500 kb for a long list of incidents with many columns. To speed performance, most browsers can accept compressed data from an application server so that the full 500 kb does not have to be sent over the wire. Instead, the browser indicates that it can accept compressed data if the server can send it. The app server then compresses the response, which transforms the 500 kb data to about 20 kb.

Compression is enabled by default on all ServiceNow application servers. The application server always sends compressed data if your browser accepts it. There are browser settings that control whether your browser accepts compressed responses.

In Microsoft Internet Explorer (IE), navigate to Tools > Internet Options. Ensure that the following two check boxes are selected in the Advanced tab.

- Use HTTP 1.1
- Use HTTP 1.1 through a proxy server

Frequently, a proxy or edge device in the environment disables gzip compression. Enabling gzip compression also speeds up the interactions.

Cache items from https locations

If you enforce an IE policy to never cache items from an https location, every interaction must refetch a large amount of JavaScript and images from the server, which affects performance. The IE option is Do not save encrypted pages to disk, and the default is off.

Diagnostics page

Administrators can use the system diagnostics page to look for root causes of platform performance issues. This page provides an overview of useful diagnostic information about a running instance and cluster nodes. Navigate to System Diagnostics > Diagnostics Page.
### System Diagnostics

#### Cluster Nodes Status
- **Name**: app124421.iad4.service-now.com:demo1nightlyhelsinki001
- **Status**: online
- **Logged in users**: 26
- **Last reported**: 0 seconds
- **Last reported (seconds ago)**: 0
- **JVM UP time**: 13 hours 1 minute
- **JVM CPU time**: 3 hours 8 minutes
- **Scheduler running**: true
- **Scheduler queue length**: 0
- **Memory (MB)**: 813.0 of 1880.0
- **JVM Classes**: 27229.0 toasted, 1503.0 unloaded
- **Transactions**: 82905
- **Errors**: 218
- **GC.ConcurrentMarkSweep.Count**: 329 (2 per 5 minutes)
- **GC.ConcurrentMarkSweep.TotalTime**: 202285 (4 minutes)
- **GC.ConcurrentMarkSweep.AvgTime**: 0.88840425
- **GC.ParNew.Count**: 7436 (47 per 5 minutes)
- **GC.ParNew.TotalTime**: 144463 (2 minutes)
- **GC.ParNew.AvgTime**: 0.019483676

#### System overview
- **Emails (recv) last 60 minutes**: 0
- **Emails (sent) last 60 minutes**: 0
- **Events pending**: 1
- **Log entries last 60 minutes**: 409
- **POP3 Status**: ?
- **SMTP Status**: There is currently no active SMTP account configured, cannot send email

#### Database overview
- **URL**: jdbc:mysql://db160144.iad4.service-now.com:3441/af5833df117db50a5
- **Name**: demo1nightlyhelsinki_1
- **Driver**: com.mysql.jdbc.Driver
- **Type**: com.mysql.jdbc.Driver
- **Version**: 5.6.16-log
- **JDBC**: 1.1
Memory

To see how much memory each node is using, you can use the 'stats' page for each node in System Diagnostics. Each 'stats' page lists the available and in-use memory. Bear in mind that memory use will fluctuate, and it's not uncommon for it to 'creep' up to beyond 95% usage before memory garbage collection reduces it back to normal levels.

Cluster Nodes

If you're running a multiple-node cluster, it's useful to know the status of each of the nodes. The nodes check in every 30 seconds and display their current status in the 'sys_cluster_state' table. You can see this information by clicking the 'Note States' module in the 'System Cluster' application.

Transactions

If you're looking for 'what was this user doing at this time', the transaction log is your friend. The transaction log lists all transactions, the user who performed it, and the URL the user was going to. You can get to the transaction log by going to System Logs > Transaction Log.

Email

The email log can help you determine whether emails are sending, who they're sending to, and the format of the message itself. The email log also shows all inbound email. You can get to the email log by going to System Logs > Email Log.

Configuring System Diagnostics Properties

Use properties to define when things appear red on the page.

Navigate to System Properties > System Diagnostics.
System Diagnostics

Please edit your changes and press Save

Customization Properties for System Diagnostics

Auto refresh the system_diagnostics_page after this many seconds:
60

Condition used to flag Emails Received value:

Condition used to flag Emails Sent value:

Condition used to flag Pending Events value:
> 1000

Condition used to flag number of log entries in last 24 hours value:

Condition used to flag a node’s Last Reporting Time value:
> 180

Condition used to flag a node’s Scheduler Is Running value:
!== 'true'

Condition used to flag a node’s Schedule Queue Length value:
> 10

Condition used to flag a node’s Status value:
!== 'online'

Condition used to flag POP3 Status value:
.indexOf('Connected') == -1

Condition used to flag SMTP Status value:
System Diagnostics Stats Tools

To aid in performance evaluation, the Stats Tools records statistics for system activities that affect performance such as the execution of queries, scripts, and transactions.

**Note:** The Stats Tools plugin is activated by default. It requires the admin role to activate or upgrade, and it requires the com.snc.jrobin.

Stats Tools adds modules under System Diagnostics > Stats, including Slow Queries, Slow Scripts, and Slow Transactions. Each module accesses a table of activity patterns [sys_query_pattern], [sys_script_pattern], and [sys_transaction_pattern]. Each pattern table represents a collection of unique activities. Each collection is an aggregation of executions of that unique activity over all time. Each record provides basic timing analysis with example identifiable details of the activity.

**Note:** To aid in debugging, you can filter most of these logs by application scope, limiting the transactions (for example, slow scripts or events) to only those transactions originating in specific scopes.

Activity patterns are immediately recorded to a cache and are later persisted to their pattern table. If you flush server caches, then recorded activities that have not been persisted are cleared. The following are examples of pattern records.

- Each time a query is executed that meets the recording and persistence threshold it is aggregated and stored as a query pattern record.
- Each time a particular business rule is executed it aggregates to a script pattern record.
- Each time a particular background job runs it aggregates into a unique transaction pattern record.
- Each click of the New button on the Incidents list counts as a list type transaction pattern with specific form action.

**Metrics**

Metrics include total and average times of interest per unique execution pattern over the total execution count. Metrics are aggregated with each new instance of the unique activity and persisted to the pattern record.

**Metadata**

Example data from specific executions are included on each pattern to identify execution details.

**Characterizations of each activity type**

<table>
<thead>
<tr>
<th>Transactions</th>
<th>Any transaction type includes server-side and related client-side transactions.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Metrics include Total server load time, which aggregates the total server-time excluding semaphore and session wait times. It also aggregates relevant server transaction times that are found on the syslog_transaction table.</td>
</tr>
<tr>
<td></td>
<td>Transaction types:</td>
</tr>
<tr>
<td></td>
<td>• An HTTP Request transaction is identified by a URL, transaction type, processor, form/list action, URL query (filters), and related table name.</td>
</tr>
</tbody>
</table>
Any other transaction is identified by its transaction URL/page/name, transaction type, and processor or thread name.

**Scripts**
Any script activity type includes scripts evaluated by GlideScopedEvaluator.

**Script Types:**
- A Jelly Script is identified by the sys_jelly_file table, jelly file path, line number, and script that was executed.
- Any other script is identified by the table and sys_id.

**Queries**
Any query activity includes prepared statements executed by GlideDBI

**Query Types:**
- All queries are identified by MongoDB query or insert, update, or select statements, as well as other components of the statement like selected columns, where clause, unions, column sets, and limits.

### Slow mutex locks record detail

Administrators can use slow mutex logs to gain insight into how mutex locks are affecting platform performance.

<table>
<thead>
<tr>
<th><strong>Field</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mutex name</td>
<td>The name of the mutex lock for this record.</td>
</tr>
<tr>
<td>Is Fast Lock</td>
<td>If false, the lock was placed on a record in the ServiceNow platform. If true, the lock was placed on a record in the underlying database.</td>
</tr>
<tr>
<td>Average execution time</td>
<td>The average time for which the mutex lock was held.</td>
</tr>
<tr>
<td>2-hour moving average (ms)</td>
<td>The average of the moving average values of execution time, calculated over periods of two hours.</td>
</tr>
<tr>
<td>Day moving average (ms)</td>
<td>The average of the moving average values of execution time, calculated over periods of one day.</td>
</tr>
<tr>
<td>Month moving average (ms)</td>
<td>The average of the moving average values of execution time, calculated over periods of one month.</td>
</tr>
<tr>
<td>Execution count</td>
<td>The number of similar occurrences that are aggregated.</td>
</tr>
<tr>
<td>Last sighting</td>
<td>The time and date the last occurrence was noted.</td>
</tr>
<tr>
<td>First sighting</td>
<td>The time and date the first occurrence was noted.</td>
</tr>
<tr>
<td>Example stack trace</td>
<td>A stack trace for an individual mutex lock.</td>
</tr>
<tr>
<td>Total execution time</td>
<td>The sum of execution time for the aggregated occurrences.</td>
</tr>
<tr>
<td>Has</td>
<td>The hash value for this record.</td>
</tr>
<tr>
<td>Label</td>
<td>The mutex lock label.</td>
</tr>
<tr>
<td>Example URL</td>
<td>The URL for an individual mutex lock.</td>
</tr>
<tr>
<td>Event Execution Time / Event Count Trend graphs</td>
<td>The Mutex Execution Time Trend graphs show the total execution time of these mutex locks over the most recent</td>
</tr>
</tbody>
</table>
Field | Description
--- | ---
| period of two hours, one day, or one month. The Mutex Count Trend graphs show the mutex lock counts over the most recent period of two hours, one day, or one month.

**Slow events log record detail**

As an administrator, you can use Slow Events logs to gain insight into how events are affecting platform performance. To aid in debugging, you can filter slow event log detail by application scope, limiting events to only those events originating in specific scopes.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event name</td>
<td>Name of the event for this record.</td>
</tr>
<tr>
<td>Queue</td>
<td>Event queue containing this event.</td>
</tr>
<tr>
<td>Event application</td>
<td>Application scope the slow event originated in. Global appears if the slow event originated in the global scope.</td>
</tr>
<tr>
<td>Execution count</td>
<td>Number of similar occurrences that are aggregated.</td>
</tr>
<tr>
<td>Average execution time (ms)</td>
<td>Average duration to execute the event in a single occurrence, in milliseconds.</td>
</tr>
<tr>
<td>Day moving average (ms)</td>
<td>Average of the moving average values of execution time, calculated over periods of one day.</td>
</tr>
<tr>
<td>Last sighting</td>
<td>Time and date the last occurrence was noted.</td>
</tr>
<tr>
<td>First sighting</td>
<td>Time and date the first occurrence was noted.</td>
</tr>
<tr>
<td>Hash</td>
<td>Hash value for this record.</td>
</tr>
<tr>
<td>Month moving average (ms)</td>
<td>Average of the moving average values of execution time, calculated over periods of one month.</td>
</tr>
<tr>
<td>Label</td>
<td>Label for the event.</td>
</tr>
<tr>
<td>Example URL</td>
<td>URL for an individual event.</td>
</tr>
<tr>
<td>Example stack trace</td>
<td>Example stack trace for an individual event.</td>
</tr>
<tr>
<td>Total execution time</td>
<td>Total sum of the event execution times for the aggregated occurrences.</td>
</tr>
<tr>
<td>Event Execution Time / Event Count Trend graphs</td>
<td>Event Execution Time Trend graphs show the total execution time of these events over the most recent period of two hours, one day, or one month. Event Count Trend graphs show the event counts over the most recent period of two hours, one day, or one month.</td>
</tr>
</tbody>
</table>

**Slow scripts log record detail**

As an administrator, you can use Slow Scripts logs to gain insight into how events are affecting platform performance. To aid in debugging, you can filter a slow script log by application scope, limiting scripts to only those scripts originating in specific scopes.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>Label assigned to the script.</td>
</tr>
</tbody>
</table>
### Slow transactions log record detail

As an administrator, you can use Slow Transactions logs to gain insight into how transactions are affecting platform performance. To aid in debugging, you can filter transaction log detail by application scope, limiting transactions to only those transactions originating in specific scopes.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average execution time (ms)</td>
<td>Average duration to execute the transaction, in a single occurrence, in milliseconds.</td>
</tr>
<tr>
<td>Execution count</td>
<td>Number of similar occurrences that are aggregated.</td>
</tr>
<tr>
<td>Total execution time</td>
<td>Total sum of the execution times for the aggregated executions of the transaction.</td>
</tr>
<tr>
<td>Average client time (ms)</td>
<td>Average duration to execute the transaction on the client, in a single occurrence, in milliseconds.</td>
</tr>
<tr>
<td>Total client time (ms)</td>
<td>Total sum of the transaction execution times for the aggregated occurrences on the client, in milliseconds.</td>
</tr>
<tr>
<td>Origin application</td>
<td>Application scope the transaction originated in. Global appears if the transaction originated in the global scope.</td>
</tr>
<tr>
<td>Example type</td>
<td>Example transaction type executed.</td>
</tr>
<tr>
<td>Example processor</td>
<td>Example processor for an individual transaction.</td>
</tr>
</tbody>
</table>

### Use a slow query log

Administrators can use slow query logs to gain insight into how queries are affecting platform performance. The Slow Queries log aggregates data for similar queries. Use slow query data to evaluate the need for new indexes, changes to existing indexes, or changes to frequent queries.

**Role required: admin**

Queries are similar when they select from the same table and query the same field in the where clause, but search for different values in the field. For example, these queries are aggregated as similar queries.

```
SELECT * FROM sys_user WHERE name="ITIL User"
SELECT * FROM sys_user WHERE name="System Administrator"
```
Aggregating similar query data allows administrators to monitor the performance impact of slow queries and of queries that occur frequently. The log reports data for similar queries where the total execution time exceeds 5 seconds.

1. Navigate to **System Diagnostics > Stats > Slow Queries**

   ![Slow Queries Table](image)

   **Query record fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example</td>
<td>An SQL statement for an individual query, before being canonicalized to aggregate it with similar queries.</td>
</tr>
<tr>
<td>Hash</td>
<td>The hash value for this record.</td>
</tr>
<tr>
<td>Example stack trace</td>
<td>A stack trace for an individual query. Lines referencing script code (includes both custom and base system code) appear in the following format: table_name.sys_id:line_number For example, this stack trace indicates a function call from line 119 of a script include. sys_script_include.105f70abc0a8010300d4d79ed1b93eb0:119 For more information, see stack traces.</td>
</tr>
</tbody>
</table>

2. Open a query record for more details.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example URL</td>
<td>The URL for an individual query, depending on how the query was called.</td>
</tr>
<tr>
<td></td>
<td>• User transactions: lists the transaction parameters.</td>
</tr>
<tr>
<td></td>
<td>For example, if a user navigates to the incident list, the URL is</td>
</tr>
<tr>
<td></td>
<td><code>/incident_list.do sysparm_query=active=true</code></td>
</tr>
<tr>
<td></td>
<td>• Scheduled jobs: lists the name of the scheduled job.</td>
</tr>
<tr>
<td></td>
<td>• Any other method: lists an empty field.</td>
</tr>
<tr>
<td>First sighting</td>
<td>The first occurrence of a similar query.</td>
</tr>
<tr>
<td>Last sighting</td>
<td>The last occurrence of a similar query.</td>
</tr>
<tr>
<td>Total execution time</td>
<td>Total execution time.</td>
</tr>
<tr>
<td>Execution Count</td>
<td>The number of similar query occurrences that are aggregated.</td>
</tr>
<tr>
<td>Average execution time (ms)</td>
<td>The average duration to execute one of these similar queries.</td>
</tr>
</tbody>
</table>

3. To see what the database is doing to retrieve the data, click **Explain Plan**.
   The query plan is reported in the **MySQL Explain Plan** related list. Use the query plan to evaluate the need for new indexes or changes to existing indexes. For more information, see **MySQL explain plan documentation**.
   This feature works on other supported databases, including MongoDB and Oracle.

4. To generate an index suggestion for a slow query, click **Index Suggestion**. For details, see **Generate an index suggestion for a slow query**.

**Index suggestions for slow queries**

The Index Suggestion Engine (ISE) can generate an index suggestion for a selected slow query. When you request an index suggestion for a slow query, the ISE analyzes the query and recommends an index that can improve the query execution time.

If you choose to use the index suggestion and create the index, the ISE continues to review the effectiveness of that index during a 14-day evaluation period. The ISE provides details on the index during the evaluation, including recommendations for managing the index.

Administrators use the ISE to:
  • Generate an index suggestion for a slow query.
  • Review index suggestions for slow queries in your instance.
  • Export an index suggestion to a non-production instance for evaluation and testing.
  • Schedule an index for creation.
  • Monitor the effectiveness of an index during the index evaluation period.
  • Test index performance (this test is an immediate performance assessment of the index).
  • Drop an index that does not optimize query performance, as recommended by the ISE.

In new and upgraded instances, the Index Suggestion Engine plugin (com.glide.index_suggestion) is activated by default.
How index suggestions work

You start the index suggestion process by requesting an index suggestion for a selected slow query. The ISE runs a daily job that collects column statistics from tables in the slow query, gathering data such as cardinality (unique columns in a table) and null/not null count.

Next, the ISE aggregates and analyzes the information collected, applies a weighted column ranking algorithm to the slow query, and generates an index suggestion for the query.

After an index suggestion is generated, you review the suggestion and determine whether to create the index for the slow query. When you create the index, the ISE provides information on the index as it moves through its life cycle.

You can track the index suggestion through three main processing stages:

**Index suggestions to review**

During this initial stage, you can review index suggestions that the ISE generated for your slow queries. You can choose to ignore a suggestion, export the index suggestion to a non-production instance for further testing, or schedule the index for creation. If the ISE successfully generates an index suggestion and you choose to schedule the index for creation, the index suggestion moves to the next processing stage. However, if the database cannot use the suggestion or the suggestion degrades query performance, the ISE recommends that you drop the index suggestion.

**Index in progress**

In this stage, the ISE creates the index and the 14-day evaluation period begins. The ISE does an hourly evaluation to determine whether the index improves or degrades the query execution time. The ISE updates the index state, including recommended actions that you can take. For example, if the index does not improve the performance of the slow query, the ISE advises that you drop the index. You can then schedule the index to be dropped from the database. During this stage, you can also choose to test index performance or accept an index, even if the ISE recommends dropping it.

**Index done**

In the last processing stage, the ISE describes the final state of the index and related processing activity. If the index improved the slow query time, the ISE changes the index state to Created and the database continues to use the index. If the index did not improve the query time and you chose to drop the index, the ISE drops the index from the database and changes the index state to Dropped.

**Index suggestion life cycle**
Processing states for index suggestions

The Index Suggestions [sys_index_suggestion] table provides state information on your indexes as they move through the three main processing stages:

- Index Suggestions > To review
- Index Suggestions > In Progress
- Index Suggestions > Done

Index Suggestions table
The ISE uses the following states to describe the processing activity for an index.

**Index suggestion states**

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index suggestions to review</td>
<td></td>
</tr>
<tr>
<td>Suggested</td>
<td>ISE generated an index suggestion for the slow query.</td>
</tr>
<tr>
<td>Drop Suggested—Unused</td>
<td>ISE recommends that you drop the index, since the database is not using the index for the slow query.</td>
</tr>
<tr>
<td>Drop Suggested—Performance Degradation</td>
<td>ISE recommends that you drop the index because the index did not improve the query time or made the performance worse.</td>
</tr>
<tr>
<td>Index in progress</td>
<td></td>
</tr>
<tr>
<td>Creation Scheduled</td>
<td>You scheduled the index for creation.</td>
</tr>
<tr>
<td>Creation in Progress</td>
<td>ISE is creating the index.</td>
</tr>
<tr>
<td>Creation Failed</td>
<td>ISE could not create the index.</td>
</tr>
<tr>
<td>Evaluating Effectiveness</td>
<td>ISE created the index and is assessing index performance during the 14-day index evaluation period.</td>
</tr>
<tr>
<td>Drop Suggested—Unused</td>
<td>ISE recommends that you drop the index from the table for which the index was created, since the database is not using the index for the slow query.</td>
</tr>
<tr>
<td>Drop Suggested—Performance Degradation</td>
<td>ISE recommends that you drop the index because the index did not improve the query time.</td>
</tr>
<tr>
<td>State</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Drop Scheduled</td>
<td>You scheduled the index to be dropped from the database.</td>
</tr>
<tr>
<td>Drop in Progress</td>
<td>ISE is dropping the index from the database.</td>
</tr>
<tr>
<td>Drop Failed</td>
<td>ISE could not drop the index. Contact Customer Service and Support for assistance.</td>
</tr>
<tr>
<td>Index done</td>
<td></td>
</tr>
<tr>
<td>Created</td>
<td>After the 14-day evaluation period, the ISE determined that the index improved query performance. Indicates that the database continues to use the index.</td>
</tr>
<tr>
<td>Ignored</td>
<td>You chose to ignore the index suggestion.</td>
</tr>
<tr>
<td>Dropped</td>
<td>ISE successfully dropped the index.</td>
</tr>
<tr>
<td>Accepted</td>
<td>You chose to keep the index even though the ISE recommended dropping it.</td>
</tr>
<tr>
<td>Superseded</td>
<td>A recent index suggestion replaced the index for the same table and slow query.</td>
</tr>
</tbody>
</table>

**Generate an index suggestion for a slow query**

Use the Index Suggestion Engine (ISE) to generate an index suggestion for a slow query.

Role required: admin

When the ISE generates an index suggestion for a slow query, it reviews query metrics and information from tables in the query. If the ISE does not have the information required to generate an index suggestion, the system displays messages informing you about the data needed. These messages typically provide links for obtaining more information, such as updated query metrics or gathering column statistics from tables in the query. Sometimes the ISE may be unable to suggest an index for the query and lets you know why the suggestion cannot be generated.

1. Navigate to **System Diagnostics > Stats > Slow Queries**.
2. In the Slow Queries table, click the query record for which the index suggestion is to be generated.
3. In the Slow Queries record, click **Suggest Index**.

If the ISE needs more information, the system may display one or more messages with details for obtaining that information. After you respond to each message, click **Suggest Index**. Repeat this process until the ISE has the information required to generate the index suggestion.

For example, the ISE may need:

- **Recent metrics**—If the system displays a message indicating that query metrics are outdated, the message provides a link for obtaining the most recent metrics.
  - Click the link to get the updated query metrics.
  - Click **Suggest Index**.

- **Column statistics**—If the column statistics do not exist for the query, the system displays a message asking you to schedule the Collect Column Stats job. You can choose to run the job at the default time when the system is less busy, or you can have the system collect the statistics immediately.
  - If you schedule the Column Stats job to run later, the ISE generates the index suggestion after it collects the column statistics. After the column stats job runs, return to the Slow Queries record and click **Suggest Index**.
  - If you choose to collect column stats immediately, the system displays the Collect Column Statistics progress indicator while it gathers column statistics. In the Slow Queries record, click **Suggest Index**.

When the ISE successfully generates an index suggestion, the Index Suggestion record for the query shows the index **State** as **Suggested**.

4. If you want to continue working with the index suggestion, select the next processing step:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Export</strong></td>
<td>Downloads the index suggestion as an .xml file so that you can export it to a non-production instance for testing and evaluation.</td>
</tr>
<tr>
<td><strong>Ignore</strong></td>
<td>Sets the index suggestion state to Ignore, which indicates that the index suggestion is not to be used. Index suggestions with an Ignore state are listed in the Index Suggestions &gt; Done view of the Index Suggestion table.</td>
</tr>
</tbody>
</table>
### Schedule creation
Opens the Schedule Index Creation window for scheduling index creation.

### Review index suggestions for slow queries
You can review index suggestions and indexes created by the Index Suggestion Engine (ISE). The ISE provides three main views of index suggestions as they move through their life cycle: index suggestions in review, index in progress, and index done.

Role required: admin

Access index suggestions from the Application Navigator or the Performance homepage.

1. Access the index suggestions for your instance:

<table>
<thead>
<tr>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From the Application Navigator</td>
<td>Navigate to System Diagnostics &gt; Index Suggestions &gt; Index Suggestions &gt; To review.</td>
</tr>
<tr>
<td>From the Performance homepage</td>
<td>If the suggestion icon indicates that one or more index suggestions are available, ( ), click it to open the Suggested Indexes window, and click View all suggested indexes.</td>
</tr>
</tbody>
</table>

**Note:** In the Suggested Indexes window, click View next to a specific table to open its index suggestion record in the Suggestion Details—Add Index form. This form is the same as the Index Suggestion form described later in this task.
2. In the Index Suggestions table, click the **Table Name** associated with the index suggestion you want to view.
3. Review the index suggestion for the selected table.

Index Suggestion fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slow query</td>
<td>The slow query for which the index suggestion was generated.</td>
</tr>
<tr>
<td>Example</td>
<td>An actual SQL statement for an individual query, before being canonicalized to aggregate it with similar queries.</td>
</tr>
<tr>
<td>Table name</td>
<td>Name of the table used in the query.</td>
</tr>
<tr>
<td>Column names</td>
<td>Names of the columns used in the query.</td>
</tr>
<tr>
<td>Index name</td>
<td>Name of the index, assigned by the ISE after the index is created.</td>
</tr>
<tr>
<td>State</td>
<td>Processing state of the index. For details, see the Index suggestion states table.</td>
</tr>
<tr>
<td>Imported</td>
<td>This box, if checked, indicates that the index suggestion was imported from a different instance for evaluation and testing.</td>
</tr>
</tbody>
</table>
4. Choose the next processing step for the index suggestion.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export</td>
<td>Downloads the index suggestion as an .xml file, which can be exported to a non-production instance for testing and evaluation.</td>
</tr>
<tr>
<td>Ignore</td>
<td>Changes the index suggestion state to ignore, which indicates the index suggestion is no longer active and available for index creation. Index suggestions with an Ignore state are listed in the <strong>Index Suggestions &gt; Done</strong> view of the Index Suggestion table.</td>
</tr>
<tr>
<td>Schedule creation</td>
<td>Opens the Schedule Index Creation window to schedule an index suggestion for creation.</td>
</tr>
</tbody>
</table>

**Export an index suggestion to a non-production instance**

You can export an index suggestion from a production instance to a non-production instance for evaluation and testing, before implementing the index on your production instance.

**Role required:** admin

This task involves exporting an index suggestion as an .xml file from your production instance and importing it to a non-production instance. You can then create the index and evaluate its performance on the non-production instance.

1. In your production instance, navigate to the Index Suggestion to be exported:
   a) Access the Index Suggestions table to review the index suggestions for slow queries.

<table>
<thead>
<tr>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From the Application Navigator</td>
<td>Navigate to <strong>System Diagnostics &gt; Index Suggestions &gt; Index Suggestions &gt; To review.</strong></td>
</tr>
<tr>
<td>From the Performance homepage</td>
<td>If the suggestion icon indicates that one or more index suggestions are available ( ), click it to open the Suggested Indexes window, and click <strong>View all suggested indexes.</strong></td>
</tr>
</tbody>
</table>

   **Note:** In the Suggested Indexes window, you can click **View** next to a specific table name to open its index suggestion record.

   b) In the Index Suggestions table, click the **Table Name** to open the index suggestion.

2. In the Index Suggestions form, click **Export**.

   The ISE downloads the index suggestion as an XML file with the file name `sys_index_suggestion_<alphanumeric identifier>.xml`. The file name has a unique alphanumeric string to differentiate it from other index suggestions.

3. In your non-production instance, navigate to **System Diagnostics > Index Suggestions > Index Suggestions > To review.**

4. In the Index Suggestions table under Related Links, click **Import Suggestions.**
5. In the Import XML form, choose the index suggestion file that you exported and click **Upload**.

After the import, the imported index suggestion appears in the Index Suggestions table on your non-production instance.

6. To continue the index evaluation process on your non-production instance, you can **schedule the index suggestion for creation** and **test index performance**.

**Schedule an index suggestion for creation**

Use the Index Suggestion Engine (ISE) to schedule an index suggestion for creation.

Role required: admin

1. Navigate to the index suggestion for the slow query:

   **Location** | **Description**
   --- | ---
   From the Application Navigator | Navigate to System Diagnostics > Index Suggestions > Index Suggestions > To review.

   From the Performance homepage | If the suggestion icon has a number ( ), click the icon to open the Suggested Indexes window, and click **View all suggested indexes**.

   **Note:** In the Suggested Indexes window, you can click **View** next to a specific table to open its index suggestion record.

2. In the Index Suggestion table, click the **Table Name** for which the index is to be created.

3. In the Index Suggestion form, click **Schedule Creation**.
4. In the Schedule Index Creation window, select the time that the index is to be created and click Create. You can schedule index creation later when your instance is less busy.

**Note:** If the index to be created involves large tables, such as the Incident or CMDB table, index creation may take up to one hour or longer.

- **Create now**—The Schedule Index Creation progress indicator window shows the progress of the index creation. When index creation is complete, click Close.
• **Create later**—If you select this option, the state changes to Create Scheduled, and the index is created at the scheduled time. After the index is created, the index state changes to Evaluating Effectiveness.

When the ISE creates the index at the selected time, it assigns an index name based on the tables used in the slow query.
5. Verify that the index was created by reviewing the index State in the Index Suggestion record or in the Index Suggestion table (System Diagnostics > Index Suggestions > Index Suggestions > In Progress). The Index Suggestion record shows the state, Evaluating Effectiveness. The ISE begins the 14-day index evaluation period.
6. During the evaluation period, you can monitor the index State in the Index Suggestion record or in the Index Suggestion table (System Diagnostics > Index Suggestions > Index Suggestions > In Progress).
Test index performance

After the Index Suggestion Engine (ISE) creates an index for a slow query, you can test the index to see if it improves the query time.

Role required: admin

This test is a quick assessment of the index and is not part of the 14-day index evaluation process. If you are evaluating an index suggestion on a non-production instance, you can run this test after creating the index to get immediate results on index performance.

Note: Index test results from your non-production instance may not necessarily predict similar performance results on your production instance.

1. Open the Index Suggestion record for the index to be tested:
   a) Navigate to System Diagnostics > Index Suggestion > Index Suggestions > In progress.
   b) In the Index Suggestions table, click the Table name for the index to be tested.

2. In the Index Suggestion record, click Test Performance to start the performance test.

3. When the Test Index Suggestion progress indicator shows that testing is complete, click Go to Result.

<table>
<thead>
<tr>
<th>Test Index Suggestion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query Execution Timer</td>
</tr>
<tr>
<td>Succeeded 100%</td>
</tr>
<tr>
<td>Go to result for final results - Succeeded in 0 Seconds</td>
</tr>
</tbody>
</table>

Go to Result Close
4. In the Query Performance Test Results form, compare the **Average with index** and **Average without index** fields to see if the index improved the query time.

In the following example, the index improved the query time. The **Forced** check box is unchecked, indicating that the database is using the index. If the check box is checked, the database was forced to use the index during the test but is not using the index outside of the test.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index Suggestion</td>
<td>Name of the index suggestion.</td>
</tr>
<tr>
<td>Created</td>
<td>Date and time this performance test was run.</td>
</tr>
<tr>
<td>Average with Index (ms)</td>
<td>Query time using the index suggestion.</td>
</tr>
<tr>
<td>Average without Index (ms)</td>
<td>Query time before using the index suggestion.</td>
</tr>
<tr>
<td>Forced</td>
<td>Check box indicating whether the database is using the index. If this box is checked, the database was forced to use the index suggestion, but only for this test. If the box is unchecked, the database is using the index.</td>
</tr>
</tbody>
</table>

5. Click the back arrow to navigate back to the Index Suggestion record for the table. The result of this index performance test does not change the index state recorded in the Index Suggestion record.

**Schedule an index to be dropped**

You can drop an index for a slow query when the index is not used by the database or does not improve query performance.

Role required: admin
During the index evaluation period, the ISE may recommend that you drop the index when the database does not use the index or the ISE finds that the index does not improve the query time. You can drop the index immediately or schedule the drop for a later time.

**Note:** If you want to retain an index even though the ISE recommends dropping it, you can use the Accept option in the Index Suggestion record to continue using the index. Before using this option, contact Customer Service and Support for guidance.

1. Navigate to **System Diagnostics > Index Suggestions > Index Suggestions > In Progress**.
2. In the Index Suggestions table, click the Table Name for the index to be dropped.
3. In the Index Suggestion record, click **Schedule Drop**.
4. In the Schedule Index Drop window, select the time you want the index dropped and click **Drop**. You can schedule the index drop at a later time, when your instance is less busy.

**Note:** If the index you want dropped involves large tables, such as the Incident or CMDB table, dropping the index may take up to one hour or longer.

- **Drop now**—The Schedule Index Drop progress indicator window shows the progress of the index drop. When the index drop completes, click **Close**. If the drop is successful, the Index Suggestion record shows the index state as Dropped.
Schedule Index Drop

- **Drop later**—When you schedule the drop, the index state changes to Drop Scheduled. When the system drops the index at the scheduled time, the index state changes to Dropped.

5. Verify that the index was dropped by reviewing the index state in the Index Suggestion record or in the Index Suggestion table (System Diagnostics > Index Suggestions > Index Suggestions > Done).

transaction call chains

Identify and debug the root causes for a problematic transaction by recording, and then reviewing, its call chain. A call chain consists of the ordered series of scripts executed during the life cycle of a transaction.

Transaction Call Chain tracking enables an administrator to register the URL of a problematic transaction for recording of the call chain during the next URL occurrence. It is helpful for diagnosing transaction performance issues.
To enable transaction call chain tracking, perform the following tasks:

1. When you find a problematic transaction on the Transaction Log or Slow Transaction list that requires debugging, select it to view its detail record. To aid in debugging, filter and group these lists by application scope, limiting transactions that appear to only those transactions originating in specific scopes.

   **Note:** To learn more about these lists, see Transaction logs and Slow transactions log record detail.
2. In the record detail form, click **Record call chain of next occurrence**, located under Related Links.
   - It designates that the next occurrence of the transaction URL should be persisted with all of its call chain information.
   - You can optionally designate a user ID so call chain recording only takes place during the next transaction occurrence for a specific user.

3. The next time a user accesses the URL, the Transaction Call Chain Register record is updated to contain a listing of the script resources executed to service the request.

4. In Transaction Call Chains, review the recorded call chain for the transaction, and then take needed actions required to debug it.
Create a transaction call chain register

Create a call chain register to record call chain information for a problematic (or slow) transaction during the next occurrence of that URL. You specify that the next occurrence of the transaction URL should be persisted with all of its call chain information.

Role required: admin

1. Navigate to the Transaction Log or Slow Transactions list, select the problematic transaction, and enable recording of the call chain.

<table>
<thead>
<tr>
<th>Type of Log</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction Log</td>
<td>a. Navigate to System Logs &gt; Transactions</td>
</tr>
<tr>
<td></td>
<td>b. To aid in debugging, filter and group the Transaction Log by application scope, limiting transactions that appear to only those transactions originating in specific scopes.</td>
</tr>
<tr>
<td></td>
<td>c. Select the problematic transaction.</td>
</tr>
<tr>
<td></td>
<td>d. In the Transaction Log Entry form, click Open Record, then click Record call chain of next occurrence, located under Related Links.</td>
</tr>
</tbody>
</table>

| Slow Transactions | a. Navigate to System Diagnostics > Stats > Slow Transactions         |
|                   | b. To aid in debugging, filter and group the Slow Transactions list by application scope, limiting transactions that appear to only those transactions originating in specific scopes. |
|                   | c. Select the problematic transaction.                                |
|                   | d. In the Slow Transactions form, click Open Record, then click Record call chain of next occurrence, located under Related Links. |

2. When the Transaction Call Chain Register appears, optionally fill in the User field.

Transaction Call Chain Register form

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>URL for the selected transaction.</td>
</tr>
<tr>
<td>Transaction Log</td>
<td>Transaction log ID created during the next occurrence of the URL. This field is empty when you first create the call chain register for a transaction.</td>
</tr>
<tr>
<td>Recorded</td>
<td>Check box that indicates if call chain recording has already taken place for this transaction.</td>
</tr>
<tr>
<td></td>
<td>• This field is empty (false) when you first create the call chain register for a transaction.</td>
</tr>
<tr>
<td></td>
<td>• true appears when the call chain is recorded during the next occurrence of the URL.</td>
</tr>
</tbody>
</table>
3. Click **Submit**.

A call chain register is created that designates that the next occurrence of the transaction URL should be persisted with all of its call chain information.

**Note:** Once the call chain is recorded (true appears in the **Recorded** field), you can view it in the Transaction Call Chain Register form itself. To learn more about transaction call chains, see Review a transaction call chain.

**Review a transaction call chain**

Use Transaction Call Chains to review the resulting call chain for a selected transaction.

Role required: admin

1. Navigate to **System Diagnostics > Transaction Call Chain > Transaction Call Chains**.
2. To view call chain detail, click the **Created** field for the selected call chain component or script.

**Note:** You can view transaction log detail by clicking the **Transaction Log** field for the selected call chain component or script. To learn more, see Transaction logs.

### Transaction Call Chain form

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Table</td>
<td>Source table for the script resource executed in the call chain.</td>
</tr>
<tr>
<td>Source</td>
<td>Script resource executed in the call chain.</td>
</tr>
<tr>
<td>Persisted Sequence</td>
<td>Order in which the script executed in the call chain.</td>
</tr>
<tr>
<td>Call Depth</td>
<td>Depth of the executed call chain.</td>
</tr>
<tr>
<td>Trigger Table</td>
<td>Name of trigger table, if any, for the executed call chain component.</td>
</tr>
<tr>
<td>Duration(ms)</td>
<td>Observed duration for the script execution, in milliseconds.</td>
</tr>
<tr>
<td>Transaction Log</td>
<td>Transaction log ID created for the recorded call chain.</td>
</tr>
</tbody>
</table>
Transaction cancellation

A user can cancel a transaction that takes longer than expected to load.

Causes of slow-loading transactions include the following scenarios.

• Sorting a large number of records by an unindexed string field.
• Grouping a large table on a field that has predominantly distinct values.
• Exporting all rows from a large table.
• Testing a poorly scripted business rule that has an infinite JavaScript loop.

Note: You cannot cancel an import with these controls.

Transaction cancel timer

During a long-running transaction, a timer and a red cancellation button appear in the banner frame.

Cancel request

To cancel the transaction, click the cancellation button. The timer indicates that the transaction is being canceled. When it is finished, you see a message that the transaction was canceled.

If the transaction completes successfully, the timer indicates how long it took for the transaction to complete.

Canceled transaction logs

Canceled transactions appear in the transaction log with CANCELLED appended to the URL. Transactions canceled by a user are logged differently from transactions canceled by Transaction quotas.
Cancel transaction properties

Administrators can configure the behavior of the transaction cancel capability using the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Definition</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.glide.request_manager.active</td>
<td>Let users cancel long running transactions (enabled by default).</td>
<td>Open the sys_properties table.</td>
</tr>
<tr>
<td>glide.ui.transaction.long_response.time</td>
<td>Delay in seconds before the cancel transaction button appears for a long-running transaction.</td>
<td>Navigate to System Properties &gt; UI Properties</td>
</tr>
</tbody>
</table>

View and kill active transaction

Administrators can view active transactions and kill long-running transactions.

**Note:** Functionality described here requires the Admin role.

This action is intended to stop background processes, such as scheduled jobs, and not user-initiated transactions.

1. If high security is enabled, elevate privileges to security_admin.
2. Navigate to the appropriate Active Transactions module.
   - To view and kill transactions on the current node for your instance, navigate to User Administration > Active Transactions.
   - To view and kill transactions on all nodes for your instance, navigate to System Diagnostics > Active Transactions (All Nodes).
3. Select the transaction you want to stop.
4. Either right-click the record and select Kill, or select the check box next the to record and select Kill from the Actions on selected rows drop-down at the bottom of the list.

Canceled-transaction logging to a table

The system logs canceled-transactions to a table in addition to the transaction log.

Transactions canceled manually or by a quota rule are logged to the Transaction Cancellation Log [syslog_cancellation]. The Transaction Cancellation Log is an extra debugging feature, and will not contain information on all cancellations.

**Note:** There are safeguards in place to prevent infinite loops and issues related to synchronicity, which mean it is not always possible to log a cancellation to a database table.

You can find the Transaction Cancellation Log by clicking System Logs > System Log > Transaction Cancellations

You can turn off canceled-transaction logging to a table by changing a property.
Canceled-transaction log property

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.quota.manager.log.cancellation</td>
<td>Indicates whether canceled transactions are to be logged to the Transaction Cancellation Log table. Type: Boolean Default value: true Location: Add to the System Properties [sys_properties] table</td>
</tr>
</tbody>
</table>

Import set performance

The algorithm transforms import sets from their staging table into their final destination.

Importing data via an import set requires two phases:

1. The data is loaded from a data source into a staging table
2. The data is transformed from the staging table into a target table

The transform algorithm operates in "blocks" of 100 records at a time as opposed to the previous algorithm which transformed a single record at a time. The newer approach allows the application server to pre-fetch a variety of information relevant to each block of records, reducing the number of unique interactions with the database and improving throughput.

Who should expect to see a performance improvement?

Any customer using import sets should expect to see a performance improvement in large transformations.

What kinds of transformations benefit the most from these changes?

Transformations with a large number of reference or choice type columns see the largest improvement.

What kind of transformations benefit the least?

Transformations that with complex or unkeyed coalesce conditions see a proportionately smaller benefit.

Thread performance monitoring

The instance tracks the performance of individual threads, which administrators can view in the transaction log or System Overview graph in the Performance homepage.

Thread performance can be monitored in two places as described in the following sections.

Transaction log

The amount of time a thread waits for an available semaphore or session synchronization is included in the Response Time field in the transaction log. To view the transaction log, navigate to System Logs > Transactions.

Performance graph

Every second, the system looks at all active threads (both UI and background) and places them into one of the following categories.
• **CPU**: The thread is active, but is not executing any of the steps. This condition typically means non-business rule compute time, although in this case a few other internal wait states are categorized as CPU. Therefore a 1:1 correlation between threads in a CPU count and hardware CPU utilization is not expected.

• **Database**: Waiting for information from the database.

• **Business Rule**: The system is running a business rule (synchronous or asynchronous) and is not currently executing a query (which would be database).

• **Network**: Writing data out to the network or waiting for an outbound network buffer to flush.

• **Concurrency**: Cannot run because they are waiting on a semaphore or session synchronization.

Every minute, the system averages these transactions and records them in the database. These averages are displayed in the **System Overview** graph available in the ServiceNow Servlet metrics. For details, see ServiceNow Servlet.

The System Overview chart can be added to any homepage. For more information, see Add existing reports to a homepage.

### Platform performance metrics

You can view a wide range of platform performance metrics for your instance and for the machine on which your instance is running. The ServiceNow Performance homepage provides central access to different graph sets for monitoring the performance of your instance.

To open the ServiceNow Performance homepage:

1. Navigate to **Self-Service > Homepage**.
2. In the homepage list, select **Diagnostics**.
3. In the Diagnostics list, select **ServiceNow Performance Data**.

The ServiceNow Performance homepage features time series graphs for analyzing system behavior and patterns over selected time periods. The homepage interface provides:

- Aggregate summaries of time series graph data
- Graph overlay capability to compare two different data sources within a single graph
- Diagnostic event overlay on each graph to highlight performance anomalies
- Zoom controls to expand each graph and view time series details

**Note:** Users accessing a custom homepage or a dashboard must have an assigned pdb_user role to view performance metric graphs. For more information, see Add existing reports to a homepage and Customize your homepage content.

The graph sets provide performance data for the following functional areas:

- Asynchronous Message Bus (AMB)
- Database
- Instance View
- MySQL Global Status
- ServiceNow Servlet
- Slow Pattern

You can also filter the data in each graph by using different measurements, such as:

- Maximum and minimum values
- Means
- Medians
Customer Service and Support uses some of these graphs to troubleshoot performance issues or help you tune your system for maximum efficiency.

**ServiceNow Performance homepage features**

The ServiceNow Performance homepage provides the following graph and display controls.
ServiceNow Performance homepage elements

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1      | Graph controls:  
  - **Graph set**: Graph collections for viewing performance in specific functional areas:  
    - AMB, Database  
    - Discovery  
    - MySQL Global Status  
    - ServiceNow Servlet  
    - Slow Pattern  
  - **Monitorable items**: Name of the instance under evaluation.  
  - **Timespan**: Period over which the data is captured: 1 hour, 2 hours, 1 day, 7 days, or 30 days  
  - **Compare with graph list**: Graph overlay feature that lets you select a graph from a different data source and compare it to the current graph set. |
| 2      | Suggestion icon: Opens the Suggested Indexes window, which provides links to index suggestions that have been created for slow queries. For details, see Review index suggestions for slow queries. |
| 3      | Display controls:  
  - **Information tooltip**: Provides details about the area on the graph you point to.  
  - **Documentation icon**: Opens the documentation page for the graph set. Appears when you point to the right corner of a graph. Opens the documentation page for the graph set.  
  - **Fullscreen icon**: Opens an enlarged view of the graph, which includes a legend that identifies the graph data. Appears when you point to the right corner of a graph. |
| 4      | Diagnostic Events widget: Lists system events that occurred during the selected timespan. Provides controls for displaying diagnostic events on graphs. |

**Display and zoom controls**

**Fullscreen graph view**

Click the fullscreen icon to open an enlarged view of a graph. The full screen view includes a legend with check boxes for controlling data displayed in the graph. To disable the display of a data item in a graph, clear its check box. On some graphs, you can also change the sort order of certain metrics in the legend.
Zoom in on a selected area of the graph

Click and drag across a portion of the graph area to zoom in on that area and view details over a smaller time interval. To return to the original view, click **Reset Zoom**.
Graph overlays

Use the graph overlay feature to look for trends or patterns between different data sets. For example, you can overlay the Database Response graph over the ServiceNow System Overview graph to determine possible correlations.

- In the **Compare with graph** list, select a performance graph to overlay the current graph set.
- To remove the graph overlay, select **None** in the **Compare with graph** list.
Diagnostic event overlays

Display controls for diagnostic events

Use the following features in the Diagnostic Events widget to control the diagnostic events overlaid on graphs:
• **Show on graphs** switch: Click to enable or disable the event overlay on the graph set. The event overlay is enabled when the switch is green. The following severity flags identify diagnostic events on the graphs:
  - I: Information
  - W: Warning
  - E: Error

• Filter: Click the filter icon to limit the events that appear on the graphs. Clear the check boxes for events you do not want displayed.

• **Clear filter**: Click to reset the filter to its default state (show all events).
Diagnostic event information

- If you enabled the diagnostic event display, point to an event in the graph to see its information.
• For quick access to details on a particular event, click the event listed in the Diagnostic Events widget to open the Event Details form.

### Event Details fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type of event.</td>
</tr>
<tr>
<td>Reported on</td>
<td>Date and time of event.</td>
</tr>
<tr>
<td>Detail</td>
<td>Additional information on the event, such as type of plugin activated.</td>
</tr>
<tr>
<td>Severity</td>
<td>Type of diagnostic event:</td>
</tr>
<tr>
<td></td>
<td>• I: Information</td>
</tr>
<tr>
<td></td>
<td>• W: Warning</td>
</tr>
<tr>
<td></td>
<td>• E: Error</td>
</tr>
<tr>
<td>Status</td>
<td>Event state:</td>
</tr>
<tr>
<td></td>
<td>• Information</td>
</tr>
<tr>
<td></td>
<td>• Open</td>
</tr>
<tr>
<td></td>
<td>• Closed</td>
</tr>
<tr>
<td>Configuration item</td>
<td>Infrastructure component, if applicable.</td>
</tr>
</tbody>
</table>
Asynchronous Message Bus (AMB)

Asynchronous Message Bus (AMB) graphs, available to view on the ServiceNow Performance homepage, use asynchronous communication to monitor the transaction count and response times, which provide a performance analysis.

If you have an admin role, you can review performance metrics. The AMB graphs are intended for use by Customer Service and Support to troubleshoot performance issues.

To view AMB graphs on the ServiceNow Performance homepage:

1. In the Graph Set list, select AMB.
2. In the Monitorable Items list, select an instance.
3. In the Timespan list, select a time period.

For details on using the graph and display controls on the Customer Service and Support Performance homepage, see Platform performance metrics.

The following graph displays the maximum, median, and minimum response times in milliseconds over a user-selected timespan. The second graph shows the number of AMB transactions over a user-selected timespan.
Database graphs, available to view on the ServiceNow Performance homepage, display metrics for various database operations, for example, insertions and deletions. They also display a current count of database connections for the selected ServiceNow instance.

If you are running on a single node, which is typical, the graphs show everything. All the traffic shown in the graphs is specific to your cluster node or instance. If you are looking at the database graph for your Discovery node, it does not include traffic for your UI node or vice versa.

If you have the admin role, you can review performance metrics. To view database metrics on the ServiceNow Performance homepage:
1. In the **Graph Set** list, select **Database**.

2. In the **Monitorable Items** list, select an instance.

3. In the **Timespan** list, select a time period.

For details on using the graph and display controls on the ServiceNow Performance homepage, see [Platform performance metrics](https://servicenow.com).
• **Database Throughput**: Displays the count (per minute) for each type of database operation (inserts, deletes, and so on) over time.

• **Database Response**: Displays the response time (in milliseconds) for each type of database operation.

• **DB Connection Use**: Shows how many connections this instance has open to the database. View the maximum, median, and minimum number of database connections in use by the selected node.

• **Replication Throughput**: Measures the difference in the data (delta) between the production instance and the replicated instance as user activity changes the database. Replication is the process whereby an entire instance is replicated on a second machine for failover protection.

    Customer Service and Support uses this information to monitor the progress of replicating a customer instance.

**Instance View**

Review data points across all near nodes (instances) using the Instance View graph set. In a single view, you can review how all active nodes are responding and identify which nodes are experiencing issues.

If you have the admin role, you can review performance metrics. Follow this procedure to view instance performance graphs on the ServiceNow Performance homepage:

1. In the **Graph Set** list, select **Instance View**.
   - The **Monitorable Items** list and **Compare With** selections are both disabled.
   - The **Monitorable Items** list has a value **-All-** for all near (active primary) instances, and excludes far (primary offline or active secondary) instances.
   - Each metric displays data across all active nodes. For example, if you have three instances, all three appear in each metric.

   **Note**: You can view performance metrics for up to 49 near nodes. If you have more than 49 nodes, no data appears for the 50th instance and above.

2. In the **Timespan** list, select a time period.

3. To overlay diagnostic events that have taken place during the time span you requested, toggle **Show on graphs, which appear** next to Diagnostic Events.

For details on using the graph and display controls on the ServiceNow Performance homepage, see **Platform performance metrics**.

Instance View
Transactions: Displays all UI transactions initiated by users. This graph can show large spikes in end-user traffic and identify when peak end-user activity occurs.
• **Response Time**: Displays the interval (in milliseconds) between the time the instance receives a transaction and the time the instance responds. Displays the time the server takes to complete a transaction, on average, during the given time span.

An increase in average response time might indicate that there is a systemic issue or an influx of generally slower transactions. To identify possible performance problems, you can correlate response time with other areas, such as memory, database, or a CPU.

• **Sessions**: Shows active sessions, including those sessions initiated by the MID Server and external integrations. Large numbers of stale but active sessions can lead to memory and performance issues. Session counts larger than 10,000 can typically result in performance degradation. Consider reviewing integration session guidelines and limiting session timeouts.

• **Session Wait Queue**: Displays the number of transactions that are waiting on another transaction for the same user. Waiting sessions occur when a user submits a duplicate request before the prior request completes. Can indicate a slow page or a transaction that requires further investigation.

To identify the transactions that are waiting, check the Transaction Log Entry [syslog_transaction] and view the Session wait time to find the transactions that are waiting. Next, find the transaction [Transaction Number?] that the user is waiting on.

• **Semaphore Use**: Shows the number of semaphores in use by the selected instance. Semaphores control the number of user transactions that can run in parallel.

Long-running transactions on a semaphore can back up all semaphores, causing transactions to wait. The platform manages semaphores, requiring no customer administration. The semaphore graph is used only for troubleshooting.

• **Semaphore Wait Queue**: Shows the wait queue for a semaphore. Use this graph with the **Semaphore Use** graph. A high wait queue indicates long-running transactions on the semaphore. A high and persistent semaphore queue can indicate that the instance node is overloaded with work.

Check the Transaction Log [syslog_transaction] to find the longest-running transactions during that time period and identify the problem. This graph is used only by the platform.

• **Scheduler Queue Length/ Scheduler Completed Jobs**: Displays all scheduler activity for the selected instance, including probes. You can determine the backlog of scheduled jobs in the queue for a particular time period. You can then compare that against the rate at which the jobs are being processed during the same period.

• **Errors**: Shows any severe errors printed to the localhost logs or syslog_ransactions. Multiple severe errors indicate a problem that requires further investigation.

• **Events Processed**: Shows the average number of events processed during the selected time period.

• **HTTP Transactions**: Displays all completed HTTP transactions, including UI, integration, and AMB traffic. This graph can show large spikes in HTTP traffic and can help identify when peak user activity occurs.

### Isolating data for specific instances

Using the Fullscreen View, you can isolate information for specific instances in a selected metric.
1. Select a metric, and then click the Fullscreen icon to open an enlarged view of the graph.
2. Clear the check box next to the instances you want to exclude.
   • For example, clear the check box next to Instance_8080 to exclude its data.
   • Only data for Instance_8081 and Instance_8082 appears.

**MySQL Global Status**

The MySQL Global Status graphs, available to view on the ServiceNow Performance homepage, provide an aggregate view of all traffic going to your database server. These graphs are distinct from the Database graph set, which monitor only queries originating at your particular application instance.

All the traffic shown in the MySQL Global Status graphs is specific to your cluster node and instance. If you have an admin role, you can review performance metrics.

The MySQL Global Status graphs are intended for use by Customer Service and Support to troubleshoot performance issues.

To view metrics for MySQL server status global variables on the ServiceNow Performance homepage:

1. In the **Graph Set** list, select **MySQL Global Status**.
2. In the **Monitorable Items** list, select an instance.
3. In the **Timespan** list, select a time period.

For details on using the graph and display controls on the ServiceNow Performance homepage, see Platform performance metrics.
**ServiceNow Servlet**

Each instance has a servlet, and you can monitor its performance using the Servlet graph set on the ServiceNow Performance homepage.

If you have the admin role, you can review performance metrics. To view servlet graphs on the ServiceNow Performance homepage:

1. In the **Graph Set** list, select ServiceNow Servlet.
2. In the **Monitorable Items** list, select an instance.
3. In the **Timespan** list, select a time period.

For details on using the graph and display controls on the ServiceNow Performance homepage, see Platform performance metrics.
• **System Overview**: Provides thread performance information. Every second, the system looks at all active threads (both UI and background) and places them into one of the following categories:

  • **CPU**: The thread is active, but is not executing any of the steps. This condition typically means non-business rule compute time, although in this case a few other internal wait states are categorized as CPU. Therefore a 1:1 correlation between threads in a CPU count and hardware CPU utilization is not expected.
  
  • **Database**: The thread is waiting for information from the database.
  
  • **Business Rule**: The system is running a business rule (synchronous or asynchronous) and is not currently executing a query (which would be database).
  
  • **Network**: The thread is writing data out to the network or waiting for an outbound network buffer to flush.
  
  • **Concurrency**: The threads cannot run because they are waiting on a semaphore or session synchronization.

The system averages these transactions every minute and records them in the database. The graph shows the averages for each category.

• **Transactions**: Displays all UI transactions initiated by users. This graph can show large spikes in end-user traffic and identify when peak end-user activity occurs.

• **Response Time**: Displays the interval (in milliseconds) between the time the instance receives a transaction and the time the instance responds. Displays the time the server takes to complete a transaction, on average, during the given time span.

An increase in average response time might indicate that there is a systemic issue or an influx of generally slower transactions. To identify possible performance problems, you can correlate response time with other areas, such as memory, database, or a CPU.

• **Sessions**: Shows active sessions, including those sessions initiated by the MID Server and external integrations. Large numbers of stale but active sessions can lead to memory and performance issues. Session counts larger than 10,000 can typically result in performance degradation. Consider reviewing integration session guidelines and limiting session timeouts.

• **Session Wait Queue**: Displays the number of transactions that are waiting on another transaction for the same user. Waiting sessions occur when a user submits a duplicate request before the prior request completes. Can indicate a slow page or a transaction that requires further investigation.

To identify the transactions that are waiting, check the Transaction Log Entry [syslog_transaction] and view the Session wait time to find the transactions that are waiting. Next, find the transaction [Transaction Number?] that the user is waiting on.

• **Semaphore Use**: Shows the number of semaphores in use by the selected instance. Semaphores control the number of user transactions that can run in parallel.

Long-running transactions on a semaphore can back up all semaphores, causing transactions to wait. The platform manages semaphores, requiring no customer administration. The semaphore graph is used only by for troubleshooting.

• **Semaphore Wait Queue**: Shows the wait queue for a semaphore. Use this graph with the Semaphore Use graph. A high wait queue indicates long-running transactions on the semaphore. A high and persistent semaphore queue can indicate that the instance node is overloaded with work.

Check the Transaction Log [syslog_transaction] to find the longest-running transactions during that time period and identify the problem. This graph is used only by .

• **Scheduler Queue Length/Scheduler Completed Jobs**: Displays all scheduler activity for the selected instance, including probes. You can determine the backlog of scheduled jobs in the queue for a particular time period. You can then compare that against the rate at which the jobs are being processed during the same period.

• **Errors**: Shows any severe errors printed to the localhost logs or syslog_ransactions. Multiple severe errors indicate a problem that requires further investigation.

• **Events Processed**: Shows the average number of events processed during the selected time period.

• **Events Logged**: Shows the average number of events queued and added to the event log in the selected time period.
- **HTTP Transactions**: Displays all completed HTTP transactions, including UI, integration, and AMB traffic. This graph can show large spikes in HTTP traffic and can help identify when peak user activity occurs.

### Slow Pattern

You can identify Slow Patterns (transactions, scripts, slow queries, events, mutexes, and cache) in your instance by using the Slow Pattern graph set on the ServiceNow Performance homepage.

If you have an admin role, you can review performance metrics. To view Slow Pattern graphs on the ServiceNow Performance homepage:

1. In the **Graph Set** list, select **Slow Pattern**.
2. In the **Monitorable Items** list, select an instance.
3. In the **Timespan** list, select a time period.

For details on using the graph and display controls on the ServiceNow Performance homepage, see [Platform performance metrics](#).

In the fullscreen view of each Slow Pattern graph, the legend provides links to the Slow Pattern records represented in the graph. For example, the legend in the Slow Query Time graph lists the slowest queries for the instance during the selected timespan.

- Clicking a slow query item in the legend opens the Slow Queries record for that item. You can review query details and determine what action to take on the slow query.
- For convenience, associated Slow Pattern graphs appears below the record so you can review and compare the graphs with details from the Slow Pattern record.
Table rotation

Table rotation preserves instance performance and averts risk associated with querying growing data sets. This feature uses the External Communication Channel (ECC) Queue and the `sys_created_on` field to separate data sets into multiple tables based on date.

**Functionality**

The administrator specifies the time parameter (duration) of the process and the number of tables (rotations) within. After the rotation writes the last table in a rotation, the rotation overwrites the first table in the rotation. Please contact ServiceNow Technical Support before applying table rotation to a custom table.

Examples:

- The query `Records created between 2015/12/10 08:49 and 2015/12/09 07/34 where topic=SystemCommand` is translated to a SQL query on a single table, because the clause on `sys_created_on` targets a single shard.

- The query `Records updated between 2015/12/10 08:49 and 2015/12/09 07/34 where topic=SystemCommand, or without a date range, needs to target all shards and therefore is translated as a union query on all shards.`

**Advantages**

- Allows deletion of old data without affecting current data (for example, to drop or truncate a table).
- Ensures tables only grow to a reasonable size.
- Reduces working set of data when date is known for query.

**Disadvantages**

Queries that do not use the table rotation date (for example, by using the `sys_created_on` field), force an inefficient union query to query time ranges that span multiple tables and can be extremely slow if the number of sub-tables is large.

To improve performance, it is recommended that the query includes a window of created dates.

You can use table rotation for sequentially-written tables or for insert-only tables. You cannot use table rotation for `sys_import` tables or tables that extend the Task `[task]` table.

**Apply table rotation**

You can apply a table rotation to preserve instance performance.

Role required: admin

1. Navigate to **System Definition > Table Rotations**.
2. Click **New**, or select the table rotation group to modify.
3. Fill in the fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the table.</td>
</tr>
<tr>
<td>Type</td>
<td>Choose Rotation, Extension, or Shard. Rotation and Extension are time-based, Shard is based on a document ID. See Database rotation for more information.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Rotations             | Sets the number of tables to maintain through the duration.  
                                        | Applies to Rotation type.                                                    |
| Duration              | Set the overall duration for the action.  
                                        | Applies to Rotation and Extension type.                                      |
| Clean base rotation   | Sets the date to clean (truncate) the base table.  
                                        | Applies to Rotation type.                                                    |
4. Click **Submit** or **Update**.

**Note:** Deleting a rotation deletes the additional tables and all the data. Do not delete the rotation if you still need the data.

When you define a new rotation, a schedule creates and new data writes to one of the tables in the rotation group. The group includes the original table plus several additional tables.
### Table Rotation Group

**syslog**

<table>
<thead>
<tr>
<th>Name</th>
<th>syslog</th>
</tr>
</thead>
</table>

**Type**

- Rotation

**Rotations**

- 8

**Duration**

- Days: 7
- Hours: 00

**Clean base rotation**

- 2021-02-12 23:22:55

### Related Links

**Synchronize shards**

### Table Rotation Schedule (9)

#### Table Rotation Schedule

<table>
<thead>
<tr>
<th>Name</th>
<th>Offline</th>
<th>Table name</th>
<th>Valid from</th>
<th>Valid to</th>
</tr>
</thead>
<tbody>
<tr>
<td>syslog0001</td>
<td>false</td>
<td>Log Entry [syslog0001]</td>
<td>2020-12-17 04:09:34</td>
<td></td>
</tr>
<tr>
<td>syslog0002</td>
<td>false</td>
<td>Log Entry [syslog0002]</td>
<td>2021-01-27 04:09:34</td>
<td></td>
</tr>
<tr>
<td>syslog0003</td>
<td>false</td>
<td>Log Entry [syslog0003]</td>
<td>2021-02-07 04:09:34</td>
<td></td>
</tr>
<tr>
<td>syslog0004</td>
<td>false</td>
<td>Log Entry [syslog0004]</td>
<td>2021-01-22 04:09:34</td>
<td></td>
</tr>
<tr>
<td>syslog0005</td>
<td>false</td>
<td>Log Entry [syslog0005]</td>
<td>2021-02-08 04:09:34</td>
<td></td>
</tr>
<tr>
<td>syslog0006</td>
<td>false</td>
<td>Log Entry [syslog0006]</td>
<td>2020-12-24 04:09:34</td>
<td></td>
</tr>
</tbody>
</table>
Table flattening
Table flattening stores a hierarchy of related tables as one table in a relational database.

Extension models
Tables such as Task and Base Configuration Item [cmdb] have a hierarchy of related tables where one or more child tables extend from a parent table. The system offers these extension models to store a table hierarchy on a relational database.

<table>
<thead>
<tr>
<th>Available extension models</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extension model</td>
</tr>
<tr>
<td>Table per class</td>
</tr>
<tr>
<td>Table per hierarchy</td>
</tr>
<tr>
<td>Table per partition</td>
</tr>
</tbody>
</table>

The extension model does not affect how the tables appear or function in the instance. All table functionality, including database views, remains unchanged by the extension model.

Table per class
The Table per class extension model stores each table of the hierarchy in its own physical table on the relational database. The physical table is named after the source table of the hierarchy and each stores a different class of records such as Change, Incident, Problem, or Task. The parent table of the hierarchy, such as Task, stores a copy of every record in its descendant tables such as Change, Incident, or Problem.

To find records in a table hierarchy, the system queries records from multiple tables and joins the results. For example, when searching for incidents that have a related problem, the system must join results from the Incident, Problem, and Task tables.

Table joins cause a performance bottleneck on relational databases. The more classes a query includes, the worse the query performance. Therefore any query for records from the top of the table hierarchy has the worst performance because it requires joining all descendant tables.

The system uses the Table per class extension model by default when creating tables. Most system tables also use the Table per class extension model as there is no performance benefit from flattening them.

Table per hierarchy
The Table per hierarchy extension model stores an entire table hierarchy in a single flat physical table on the relational database. The physical table is named after the parent table of the hierarchy, such as Task. The physical table contains all records of the table hierarchy and assigns a class name column value to each descendant table of the hierarchy. The system uses the name of the source table as the class name value. For example, Task records can have class names such as Change, Incident, or Problem.

To find records in a table hierarchy, the system queries the physical table and uses the class name column to constrain the results. Since such queries do not require joining results from multiple tables, the system provides better search performance.
The system uses the Table per hierarchy extension model for the Task table hierarchy on MySQL databases. Other tables use the Table per class extension model because there is no performance benefit to flattening them. To use Table per hierarchy on an Oracle database, contact Technical Support.

**Table per partition**

The Table per partition extension model stores an entire table hierarchy in a single flat logical table on the relational database. Each logical table can have multiple physical storage tables called partitions supporting it. Each partition optimizes the database resources available to a physical table such as the column count, index count, and row size. The system adds a partition whenever the logical table needs additional relational database resources.

Each logical table is named after the parent table of the hierarchy, and each supporting physical partition consists of the logical name plus a partition name. For example, the Base Configuration Item [cmdb] table starts as a logical table with no partitions. Suppose your hardware configuration items consume enough database resources that the system creates a partition called `cmdb$par1` to store them. Later, computer configuration items could consume enough database resources to warrant the system creating a second partition called `cmdb$par2` to store these records.

Within each logical table, the system assigns a class name column value to each descendant table of the hierarchy. For example, within the Base Configuration Item logical table there are records with class names for Application, Computer, and IP Router. The system also assigns a two-digit class path value to each descendant table of the hierarchy. The class path is based on the table location in the hierarchy. For example, the parent class Hardware might have a class path such as `/!!/ID` and the child class Computer might have a class path such as `/!!/ID/!!`.

To find records in a table hierarchy, the system queries the logical table and its partitions and uses the class path column to constrain the results. Since these queries do not require joining results from multiple tables, the system provides better search performance. In addition, the class path reduces the total number of records to search, which further improves search performance.

The system uses the Table per partition extension model for the Base Configuration Item [cmdb] table hierarchy on MySQL databases. To use Table per partition on an Oracle database, contact Technical Support.

**View a table hierarchy and the extension model**

The extension model used by a table is not immediately apparent. While a hierarchy can use a single physical table, the platform displays tables as if each logical table has a unique physical table. For example, when specifying a table for a workflow, you can select Change [change_request] or Incident [incident] even though the parent table, Task [task], uses a single physical table.

Role required: admin

Administrators can view the status of flattened table hierarchies, but cannot flatten additional hierarchies. You can configure the form to add the **Extension model** field if necessary.

1. Navigate to **System Definition > Tables**.
2. Select a table record.
3. Review the **Extension model** field value, which indicates whether the table hierarchy uses multiple unique tables or a single flat table.

- **None**: Indicates that the table uses the table per class model. Defines a unique physical table per logical table in a hierarchy. For example, there are separate physical tables for Task [task], Incident [incident], Problem [problem], and Change [change_request] on the MySQL database.

**Note:** If a table has an empty Extension Model field, it is not necessarily a Table Per Class table. If the table extends another table, it actually inherits the model from any parent tables it is extending, and only when none of the parents have a defined extension model is the table’s extension model Table Per Class. This can be seen on many tables that extend the Task table. Incident is a logical table that extends Task and is physically located on Task, but by default has a blank Extension Model value.
When a table that doesn’t extend anything at all, and has a blank Extension Model field, it is a Table Per Class table.

- **Table per hierarchy**: Defines a single physical table per logical table hierarchy. For example, there is a single Task [task] table on the MySQL database that contains all the Task, Incident, Problem and Change records. This single physical table is represented as separate logical tables.

### Add a module to test connection speed

A connection test can indicate the connection speed between your computer and your instance. A connection speed test (/connection_test.do) is available as a UI page.

Role required: admin

![Connection Test](image)

Connection test is used to determine the type of connect between the end computer and your Service-now.com instance.

To start the connection test, press this **button**:

**Start Connection Test**

Average time: 594ms (per 170k)
Estimated connection:T1/Cable (average download was 282K/s)

Connection Test page

1. Perform the appropriate action for your version of the UI:

| UI16 | a. Navigate to **System Definition > Application Menus**.  
| | b. Open the application menu to which you want to add the module, for example, **System Diagnostics**.  
| UI15 | Right-click an application menu, such as **System Diagnostics**, and select **Edit Application Menu** or click the pencil icon.  

2. Click **New** in the list of modules.
3. Complete the Module form using the following values:
   • **Title**: Unique name such as **Connection Test**
   • **Link type**: URL (from Arguments)
   • **Arguments**: `connection_test.do`

   ![Module form with filled values](image)

4. Click **Submit**.

**Transaction quotas**

Transaction quotas allow you to define a quota policy for different types of transactions. A transaction quota cancels any transaction in violation of the policy and notifies the user of the cancellation.

The Transaction Quotas plugin is active by default on all new and upgraded instances.
Transaction canceled

The transaction quota also writes the cancellation message to the log file as a warning.

Transaction canceled log

Typically, administrators set transaction quotas to prevent poorly performing queries and scripts from consuming system resources. This ensures that no transaction consumes enough resources to prevent other transactions from running. Administrators can also view cancellation log messages to identify transactions that might consume excessive resources.

How transaction quotas work

Transactions use the Quota Manager, which is a background thread that cancels transactions. The Quota Manager performs the following actions.

1. Obtains a list of active transactions, similar to the list under User Administration > Active Transactions.
2. Cycles through each transaction and checks all quota rules with conditions matching the transaction. The first occurrence that exceeds any of the quota limitations triggers a transaction cancellation. If a transaction changes or there is a new quota rule, the Quota Manager re-evaluates the transaction.

**Note:** The *Order* field on a quota rule affects the order in which the quota rules are checked. The Quota Manager checks lower-order rules first (for example, order 80 before order 90), but ultimately checks all rules. This might have marginal performance implications, depending on the conditions of the rules involved.

3. Cancels the transaction if it has been running longer than the specified quota maximum.

4. Logs the running transactions.

5. Sleeps until the next heartbeat, which is controlled by the `glide.quota.manager.heartbeat` system property.

**Transaction cancellation examples**

Transactions can be canceled for more than one reason. Look for the following indicators.

- **maximum execution time exceeded**: This message appears when the `glide.quota.manager` threads cancels the transaction.
- **canceled by other transaction**: This message appears when the transaction was canceled by the session thread that initially issued it, and not by the `glide.quota.manager` thread.
- **canceled by user request**: This message appears when the user clicked the red X button to cancel the running transaction.

If you are looking for transactions that were canceled by `glide.quota.manager`, search for the `[Message] [Contains] [maximum execution time exceeded]` combination. For example:

```
Cancelling transaction /home.do - Default-thread-11.0 (maximum execution time exceeded): Thread Default-thread-11.0 (Default-thread-11.0, F530DD111B11111111FC031767DA158E), after 30000ms
```

**Add variable information to the cancellation message**

You can use the following methods of the `jvar_transaction` variable to add information to the cancellation message.

### Adding Variable Information to the Cancellation Message

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>getURL()</code></td>
<td>Returns the URL for the transaction.</td>
</tr>
<tr>
<td><code>getReason()</code></td>
<td>Returns the reason for page cancellation, localized to the user's language.</td>
</tr>
<tr>
<td><code>getQuotaId()</code></td>
<td>Returns the sys_id of the quota rule.</td>
</tr>
<tr>
<td><code>getQuotaName()</code></td>
<td>Returns the name of the quota rule.</td>
</tr>
<tr>
<td><code>getRunTime()</code></td>
<td>Returns the total run time for the page up to this point.</td>
</tr>
<tr>
<td><code>getType()</code></td>
<td>Returns the type of transaction, such as form, list, report, other.</td>
</tr>
<tr>
<td>Method</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------------------------------</td>
</tr>
<tr>
<td>getUser()</td>
<td>Returns the sys_id of the user.</td>
</tr>
<tr>
<td>getHomepage()</td>
<td>Returns the sys_id of the homepage.</td>
</tr>
<tr>
<td>getHomepageWidget()</td>
<td>Returns the name of the homepage widget.</td>
</tr>
</tbody>
</table>

## Transaction quota properties

An administrator can add the following system properties to manage transaction quotas.

### Configuring Transaction Quota Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.quota.manager.heartbeat</td>
<td>The number of seconds between the start of each Quota Manager heartbeat. This value determines how often the Quota Manager checks for transactions that exceed a quota and how often it writes status in the log file. Type: Integer Default value: 1 Location: Add to the [sys_properties] table</td>
</tr>
<tr>
<td>glide.quota.manager.minimum_transaction_time</td>
<td>The minimum number of seconds a transaction must run before the Quota Manager matches it to a transaction quota. ServiceNow recommends setting this value to at least 1 second to avoid performance issues. For optimal performance, set this value to the value of your most restrictive quota. For example, if your most restrictive quota cancels transactions longer than 1 minute, set the minimum transaction time to 60 seconds. Type: Integer Default value: 1 Location: Add to the [sys_properties] table</td>
</tr>
<tr>
<td>glide.quota.manager.debug</td>
<td>Controls whether to display (true) or hide (false) additional debugging information related to the Quota Manager. Debugging information includes running transactions, canceled transactions, and what quotas are matched to transactions. Type: True</td>
</tr>
</tbody>
</table>

### Enable transaction quota debugging

You can enable the logging of transaction quota debugging information by enabling the system property.

Role required: admin

1. Add the glide.quota.manager.debug system property, and set the value to true.
2. Navigate to System Diagnostics > Session Debug > Debug Quotas.
The Debug Quota script runs to enable debugging.

After setting the above system property to **true**, go to your system log to see messages from the Quota Manager.

**Default quota rules**

Various transaction quota rules are available in the base system.

**Fix Script Processor**

Allows the fix script processor to run for four hours.

**Presence**

Cancels presence requests quickly when the system is busy.

**REST Import Set API request timeout**

Prevents inbound REST Import Set API transactions from running for longer than 60 seconds.

**REST Table API request timeout**

Prevents inbound REST Table API transactions from running for longer than 60 seconds.

**AMB Transactions**

Cancels AMB transactions lasting longer than the specified maximum duration. Applies to all AMB transaction types: message send and message receive.

**Reference Completer**

 Stops the reference completer transaction after five seconds.

**REST Aggregate API request timeout**

Prevents inbound REST Aggregate API transactions from running for longer than 60 seconds.

**Homepage Widgets**

Prevents all homepage widgets from running longer than 30 seconds.

**REST Attachment API request timeout**

Prevents inbound REST Import Set API transactions from running for longer than 60 seconds.

**UA Count Persistor Quota**

Prevents UA count persistor scheduled jobs from running for more than one hour.

**UI Transactions**

Cancels UI transactions that are two seconds away from the 5-minute server disconnect. ServiceNow datacenter load balancers display an internal server error (HTTP Error 500) to users after five minutes. This quota rule returns a transaction canceled page instead of an error. This rule includes an exception to prevent the cancellation of background scripts.

**PA Diagnostics All**

Prevents any Diagnostics transaction that originates outside the scope of the Diagnostics application from running longer than 30 minutes. Diagnostics transactions refer to executing a diagnostic, opening a Diagnostics form, or opening a Diagnostics list.
Normal transaction activities

Before setting transaction quotas, navigate to User Administration > Active Transactions to review the normal transaction activities for your instance. You can view and terminate long-running transactions if necessary. Over time, you can determine the normal transaction load for your instance and set your quotas to match these norms.

Configure a transaction quota rule

Transaction quota rules allow you to define a quota policy for different types of transactions.

Role required: admin

Transaction quota rules allow you to specify the following conditions.

- The conditions under which the policy applies.
- The order in which transaction quotas apply.
- The maximum duration of a transaction before the quota manager cancels it.

**Warning:** Setting transaction quotas too low can severely impact your users and prevent normal instance operations. Test your transaction quotas rigorously before implementing them in production.

1. If necessary, activate the Transaction Quotas plugin.
2. Navigate to System Definition > Quota Rules.
3. Click New.
4. Complete the form.

### Transaction quota rule fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name to identify the rule.</td>
</tr>
<tr>
<td>Active</td>
<td>A check box that determines if this rule is active (selected).</td>
</tr>
<tr>
<td>Maximum Duration</td>
<td>The number of seconds a transaction has to complete before the quota cancels the transaction.</td>
</tr>
<tr>
<td>Maximum Business Rules</td>
<td>The number of business rules executions allowed.</td>
</tr>
<tr>
<td>Maximum Database Time</td>
<td>The total number of seconds for all SQL requests.</td>
</tr>
<tr>
<td>Maximum SQL Statement Time</td>
<td>The number of seconds a SQL statement can run.</td>
</tr>
<tr>
<td>Maximum Outbound Requests</td>
<td>The number of outbound HTTPs requests allowed.</td>
</tr>
<tr>
<td>Order</td>
<td>A number that represents the priority of the quota transaction in relation to other quotas. The transaction quota with the lowest timeout, the lowest order value, and matching conditions determines the applied quota policy.</td>
</tr>
<tr>
<td>Maximum Events</td>
<td>The number of sysevent inserts allowed.</td>
</tr>
<tr>
<td>Maximum Jobs</td>
<td>The number of sys_trigger inserts allowed.</td>
</tr>
<tr>
<td>Maximum SQL Queries</td>
<td>The number of SQL queries allowed.</td>
</tr>
<tr>
<td>Maximum Outbound Request Duration</td>
<td>The number of seconds for an outbound HTTP request.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the transaction quota rule.</td>
</tr>
</tbody>
</table>
5. Set a condition to specify when the transaction quota should take effect.

The transaction quota rule condition builder displays conditions that are only applicable to transactions as listed in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>The URL of the page.</td>
</tr>
<tr>
<td>Thread Name</td>
<td>The name of the execution thread that is running the transaction. Foreground threads have names like http-bio-8080-exec-1. Background threads can have various names, and are useful where the URL is not sufficiently descriptive.</td>
</tr>
<tr>
<td>Foreground</td>
<td>Whether the transaction was completed in the foreground or background:</td>
</tr>
<tr>
<td></td>
<td>• True: a foreground transaction.</td>
</tr>
<tr>
<td></td>
<td>• False: a background transaction.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of transaction:</td>
</tr>
<tr>
<td></td>
<td>• List: Any list transaction, such as incident_list.do.</td>
</tr>
<tr>
<td></td>
<td>• Form: All forms, UI pages, CMS pages, and so on.</td>
</tr>
<tr>
<td></td>
<td>• XMLHttp: Transactions that run through GlideAjax, where the URL is xmlhttp.do.</td>
</tr>
<tr>
<td></td>
<td>• Report: The page sys_report_template.do.</td>
</tr>
<tr>
<td></td>
<td>• SOAP: SOAP transactions.</td>
</tr>
<tr>
<td></td>
<td>• Export: When a list is exported in a format such as XML or Excel.</td>
</tr>
<tr>
<td></td>
<td>• Scheduler: When a scheduled job is performed.</td>
</tr>
<tr>
<td></td>
<td>• Text Search: The text search transaction or any of its related operations.</td>
</tr>
<tr>
<td></td>
<td>• Other: Any type that does not meet the qualities of another type.</td>
</tr>
<tr>
<td>User</td>
<td>The user performing the transaction.</td>
</tr>
<tr>
<td>Homepage</td>
<td>The homepage that is running. This condition is populated only if the URL is home.do.</td>
</tr>
<tr>
<td>Homepage Widget</td>
<td>The widget that is rendered in the transaction. When a homepage or non-responsive dashboard renders, each widget renders in parallel. When a responsive dashboard renders, each widget renders in sequence. When the quota is exceeded, users see the message: Widget cancelled – maximum execution time exceeded. Increase the quota value if you don’t want to show this message.</td>
</tr>
</tbody>
</table>

Note: Match the transaction quota Type to the transaction type listed in the Quota Manager log entry for the transaction.
6. Click Submit.

**View a canceled transaction**

The Quota Manager logs each canceled transaction as a warning message in the system log.

Role required: admin

Use the following procedure to search for transaction warnings in the system log.

1. Navigate to **System Logs > System Log > Warnings**.
2. Edit the filter to add the condition `[Message] [starts with] [Cancel].`
3. Click **Run**.

**Example system log messages**

An example of system log messages for transactions.

- At every heartbeat interval, which is one second by default, the Quota Manager prints the running transactions:

```
2012-02-13 12:34:08 (096) glide.quota.manager SYSTEM URL= /incident_list.do?
sysparm_userpref_module=b55fbec4c0a80090088e83d7ff500de&active=true&sysparm_query=active=true^EQ,
THREAD= http-bio-8080-exec-3, FG= true, TYPE= 1, STATE= 2, USER= null, TIME= 8,807, MEM= 0, ATTRIBUTES= {}
```

- Every time the Quota Manager matches a quota to a transaction, it prints a message similar to the following example:

```
2012-02-13 13:25:31 (900) glide.quota.manager SYSTEM QuotaFinder: Assigning quota "TEST PROBLEM FORM" with filter: type= form ^urlLIKEsys_id=46fb9e31a9fe198101492060c2a4f8cb^EQ to transaction: URL= /problem.do?sys_id=46fb9e31a9fe198101492060c2a4f8cb,
THREAD= http-bio-8080-exec-1, FG= true, TYPE= 1, STATE= 4, USER= null, TIME= 1,121, MEM= 0, ATTRIBUTES= {}
```
Every time the Quota Manager cancels a transaction, it prints a message similar to the following example:

```
2012-02-13 13:25:33 (930) glide.quota.manager SYSTEM WARNING *** WARNING ***
Transaction: Cancelling transaction /problem.do (maximum execution time exceeded):
Thread http-bio-8080-exec-1
```

**Modify the transaction cancellation page**

The Quota Manager uses a UI page to control the contents of the transaction cancellation message. 

Role required: admin

Knowledge of Apache Jelly is highly recommended when modifying the UI page. See Extensions to Jelly syntax for more information.

1. Navigate to System UI > UI Pages.
2. Open the UI page with the name `transaction_canceled_quota`.
3. In the HTML field, add or modify the new cancellation message.
   The following table describes available variables.

   **Cancellation message variables**

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>getURL()</td>
<td>Returns the URL for the transaction.</td>
</tr>
<tr>
<td>getReason()</td>
<td>Returns the reason for page cancellation, localized to the user's language.</td>
</tr>
<tr>
<td>getQuotaId()</td>
<td>Returns the sys_id of the quota rule.</td>
</tr>
<tr>
<td>getQuotaName()</td>
<td>Returns the name of the quota rule.</td>
</tr>
<tr>
<td>getRunTime()</td>
<td>Returns the total run time for the page up to this point.</td>
</tr>
<tr>
<td>getType()</td>
<td>Returns the type of transaction, such as form, list, report, other.</td>
</tr>
<tr>
<td>getUser()</td>
<td>Returns the sys_id of the user.</td>
</tr>
<tr>
<td>getHomepage()</td>
<td>Returns the sys_id of the homepage.</td>
</tr>
<tr>
<td>getHomepageWidget()</td>
<td>Returns the name of the homepage widget.</td>
</tr>
</tbody>
</table>

4. Click Update.

**Application quotas**

You can set a limit on the number of events or jobs that can run in an application’s scope within a specified time.

Application quota rules set application quotas. Each scoped application can have one application quota rule. When an application exceeds the quota limit, all transactions running in the application scope are canceled. New transactions are canceled when they start until the next update period. These actions effectively block transactions from an application scope from running for the update period.

An application quota rule applies to transactions created by all instances of an application and all transactions created by methods of the application called by other applications.
If two users are running the same application, the application quota rule does not distinguish between transactions for each instance of the application. If, together, they violate the quota, all transactions in the application's scope are canceled.

If you check the Log Only option, transactions are not canceled by a quota violation. Instead, entries are added to the local host log that indicate the transactions are running under violation.

Transaction and application quota rules are evaluated separately, by defining an application quota rule, you simply introduce another restriction. A transaction is canceled if it violates a transaction quota rule, or if collectively with other application transactions, it violates its application quota rule.

You cannot define an application quota rule for the global application.

### Application-quota property

An administrator can add a system property to specify how often application quota rules are evaluated.

#### Property

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| glide.quota.manager.cluster.update.seconds    | Indicates the application quota update period in seconds. If this value is less than the glide.quota.manager.heartbeat property, the glide.quota.manager.heartbeat value is used. Type: Number  
| Default value: 300 (5 minutes)                 | **Location:** [Add to the System Properties](#) [sys_properties] table                                                                                                                                 |

#### Configure an application-quota rule

You can configure an application-quota rule to limit the number of events or jobs that can run in an application's scope within a specified time.

Role required: admin

You must be in the application scope of the application for which you want to create a rule.

1. Navigate to System Definition > Application Quota Rules.
2. Click New.
   The Application Quota Rule form is shown.
3. Fill in the fields.

#### Configuring application quota rules

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name to identify the rule.</td>
</tr>
<tr>
<td>Application</td>
<td>The scoped application's name. To change this field, use the application picker to change the application. This field cannot be Global.</td>
</tr>
<tr>
<td>Order</td>
<td>A number that represents the priority of the quota transaction in relation to other quotas.</td>
</tr>
<tr>
<td>Active</td>
<td>A check box that determines if this rule is active (selected).</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Log only | When checked, transactions are not canceled by a quota violation, but entries are added to the local host log that indicate the transactions are violating the quota rule. An entry is added to the Transaction Cancellation Log where the log only field is set.
Maximum Events | The maximum number of events allowed during the update period.
Maximum Jobs | The maximum number of jobs allowed during the update period.
Condition | The conditions that determine when the transaction quota applies. The condition builder displays conditions that are only applicable to transactions. For example, Foreground is true.
Description | A description of the transaction quota.

4. Set a condition to specify when the application quota rule should take effect.

The application quota rule condition builder displays conditions that are only applicable to transactions as listed in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attributes</td>
<td>Miscellaneous attributes that are related to the transaction.</td>
</tr>
<tr>
<td>Created</td>
<td>When the transaction was created.</td>
</tr>
<tr>
<td>Created by</td>
<td>Who created the transaction.</td>
</tr>
<tr>
<td>Foreground</td>
<td>Whether the transaction was completed in the foreground or background:</td>
</tr>
<tr>
<td></td>
<td>• True: a foreground transaction.</td>
</tr>
<tr>
<td></td>
<td>• False: a background transaction.</td>
</tr>
<tr>
<td>Homepage</td>
<td>The homepage that is running. This value is populated only if the URL is <code>home.do</code>.</td>
</tr>
<tr>
<td>Homepage Widget</td>
<td>The homepage widget that is rendered in the transaction. When a homepage is rendered initially, each homepage widget is rendered in parallel.</td>
</tr>
<tr>
<td>Initial Scope Name</td>
<td>Scope where the method that created the transaction is defined. Setting this name to anything other than the selected application means that the rule is never used. The rule only looks at transactions of the selected application, and this value has the rule look for a different application, so the condition is never satisfied.</td>
</tr>
<tr>
<td>Scope Name</td>
<td>Scope of the application that called the method that created the transaction.</td>
</tr>
<tr>
<td>Sys ID</td>
<td>A sys_id of the transaction.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Thread Name</td>
<td>The name of the execution thread that is running the transaction. Foreground threads have names like http-bio-8080-exec-1. Background threads may have various names, and may be useful where the URL is not sufficiently descriptive.</td>
</tr>
</tbody>
</table>
| Type          | The type of transaction:
|               |   • List: Any list transaction, such as incident_list.do.  
|               |   • Form: All forms, UI pages, CMS pages, and so on.  
|               |   • XMLHttpRequest: Transactions that run through GlideAjax, where the URL is xmlhttp.do.  
|               |   • Report: The page sys_report_template.do.  
|               |   • SOAP: SOAP transactions.  
|               |   • Export: When a list is exported in a format such as XML, Excel.  
|               |   • Scheduler: When a scheduled job is performed.  
|               |   • Text Search: The text search transaction or any of its related operations.  
|               |   • Other: Any type that does not meet the qualities of another type.                                                                 |
| URL           | The URL of the page.                                                                                                                          |
| Updated       | When the transaction was updated.                                                                                                             |
| Updated by    | Who updated the transaction.                                                                                                                  |
| Updates       | What was updated.                                                                                                                             |
| User          | The user performing the transaction.                                                                                                          |

5. Click **Submit**.

**Use table extension**

This example shows you how to set the Table Extension parameter to a table rotation group.

Role required: admin

**Note:** Deploy this plugin in partnership with a ServiceNow representative.

Administrators typically specify the time parameter (duration) of the process, but may alternatively specify the number of tables (rotations). After the last table in a rotation is written, new tables are added and old tables are archived. Using table extension, tables are never overwritten.

An advantage of table extension is to partition data across tables. It also allows you to archive data while ensuring that tables stay reasonably-sized. The working set of data is reduced when a date is known for the query.

The disadvantage is that table extension requires a union query when you query for a time range that spans multiple tables. Union queries are less efficient than queries against a single table.
A good practice is to use table extension when you have sequentially-written tables or insert-only type tables (there are exceptions to this parameter). Table extension is also useful in tables where data is needed for long periods of time.

The following example describes how to set table extension for the [sys_audit] table.

1. Navigate to **System Definition > Table Rotations**.
2. Click **New**.
3. Enter the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the table to apply the action. In this example, the table is [sys_audit].</td>
</tr>
<tr>
<td>Duration</td>
<td>Enter the overall duration for the action. 30 days is the duration in this example.</td>
</tr>
<tr>
<td>Type</td>
<td>Select <strong>Extension</strong>.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.
Platform security

Security is built into all levels of the Now Platform. Implement the security features that are appropriate for your organization, from managing failed logins and encrypted password protection, to access control rules and audit logs.

Platform security resources

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Security Best Practice Guide on the Customer Success Center</td>
<td>Start here for guidance on security configurations, including baseline security, authentication and authorization, encryption, and MID Server settings. You can also learn about:</td>
</tr>
</tbody>
</table>
|                                                                         | • Security responsibilities between you and ServiceNow  
|                                                                         | • Security-related certificates and certifications that ServiceNow holds  
|                                                                         | • Security contact details  
|                                                                         | • Software updates  
|                                                                         | • Mobile application security  
|                                                                         | • Vulnerability assessment and penetration testing  
|                                                                         | The ServiceNow® infrastructure and Now Platform® are intentionally built and operated with high levels of baseline security; however, as a customer you must make some decisions about the way in which your instance is configured to comply with your organization's security policies. |

Instance Security Hardening Settings

The Instance Security Hardening Settings content contains detailed descriptions, and compliance values, for the security-related system properties and plugins in the Now Platform®.

Instance Security Hardening Settings includes many of the same settings that appear in the security-related setup topics that follow. Where applicable, each setup topic includes links to helpful security information in Instance Security Hardening Settings.

Platform security features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Status</th>
<th>Top Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Security Settings</td>
<td>High Security Settings refer to several security options available in your instance.</td>
<td>Active</td>
<td>• Request High Security Settings activation</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Status</td>
<td>Top Tasks</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Certificates</td>
<td>Your instance requires certificates to establish secure connections and validate signatures.</td>
<td>Active</td>
<td>• Upload a certificate to an instance</td>
</tr>
<tr>
<td>Login and authentication security</td>
<td>Configure login security options to control access to your instance.</td>
<td>Active</td>
<td>• Define login scenarios</td>
</tr>
<tr>
<td>Web service security</td>
<td>Enforce security using basic authentication, mutual authentication, or WS-Security.</td>
<td>Active</td>
<td>• Setting up mutual authentication</td>
</tr>
<tr>
<td>Access control list rules</td>
<td>Rules for access control lists (ACLs) restrict access to data by requiring users to pass a set of requirements before they can interact with it.</td>
<td>Active</td>
<td>• Create an ACL rule</td>
</tr>
<tr>
<td>HTML sanitizer</td>
<td>Remove unwanted code and protect against security concerns such as cross-site scripting attacks by sanitizing HTML markup in HTML fields and translated HTML fields.</td>
<td>Active</td>
<td>• Enable HTML sanitizer</td>
</tr>
<tr>
<td>Auditing</td>
<td>Track record changes on auditing-enabled tables. By default, the system tracks changes to the incident, change, and problem tables, among others.</td>
<td>Active</td>
<td>• Enable auditing for a table</td>
</tr>
<tr>
<td>Domain separation for service providers</td>
<td>With domain separation you can separate data, processes, and administrative tasks into logically defined domains.</td>
<td>Requires a separate subscription.</td>
<td>• Request domain separation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Domain separation setup and administration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Domain separation and Column Level Encryption Support</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Domain separation in Edge Encryption</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Status</td>
<td>Top Tasks</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Virtual Private Network (VPN) | Use a virtual private network (VPN) to integrate your instance with external data sources over the Internet. | Available by request from ServiceNow personnel. | • Virtual Private Network (VPN)  
• Request a VPN service |
| Encryption support            | Column Level Encryption (CLE) contexts permit and deny access to encrypted data based on user role. | Active                  | • Set up encryption contexts  
• Domain separation and Column Level Encryption Support  
• Manually encrypt and decrypt MID Server attributes |
| Platform Encryption           | Platform Encryption utilizes the Key Management Framework (KMF) to enable you to fully customize and manage how fields and attachments are encrypted and decrypted on your instance. | Requires a separate subscription. | • Platform Encryption  
• Migrating to Platform Encryption  
• Platform Encryption examples |
| Key Management Framework (KMF)| Key Management Framework (KMF) API/UX lets you fully customize and manage how cryptographic operations are performed on your ServiceNow instance. | Active                  | • Understanding the Key Management Framework  
• Cryptographic module overview  
• Cryptographic purpose, algorithms, and key information  
• Key management actions |
| Database encryption and full-disk encryption | Database Encryption enables all data to be protected with symmetric AES-256 encryption, whether the database is online or offline. | Requires a separate subscription. | • Database encryption and full-disk encryption  
• Database Encryption with Customer-Controlled Switch (DBE with CCS)  
• Request database key rotation |
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Status</th>
<th>Top Tasks</th>
</tr>
</thead>
</table>
| Data Classification   | Data Classification enables support for:  
  • Visibility into the types of data hosted on Now Platform Now Platform instances.  
  • Compliance with privacy laws, and meeting regulation requirements for industries such as financial services and medical device manufacturing. | Active  | • Data Classification  
  • Components installed with Data Classification demo data  
  • Analyze data classifications using the Overview dashboard  
  • Domain separation and Data Classification |
| Edge Encryption       | ServiceNow® Edge Encryption™ encrypts sensitive data on your company premises before sending it over the Internet to your ServiceNow instance (encrypted in flight), where it remains encrypted at rest. | Requires a separate subscription. | • Edge encryption installation  
  • Edge Encryption configuration  
  • Domain separation in Edge Encryption |
| System logs           | View warnings and errors for instance processes, records, and non-critical events, such as memory usage on the server machine.                                                                         | Active  | • Transaction logs  
  • Event logs                                                                                   |
| Antivirus Scanning    | Use Antivirus Scanning to help protect your instance against virus infections that can be introduced by file attachments to your system records, such as incidents, problems, and stories.                    | Active  |                                                                                                 |

**Instance Security Hardening Settings**

The Instance Security Hardening Settings content contains detailed descriptions and compliance values for the security-related system properties and plugins in the Now Platform. You can set most of these properties in the Hardening Compliance Configuration page in the Instance Security Center.

**Overview and purpose**

The Instance Security Center calculates a Daily Compliance Score, expressed as a percentage. It is based on how compliant your current instance security settings are with the compliance values in Instance Security Hardening Settings.
Using its Hardening Compliance Configuration page, you can manage the specific security configuration settings that may affect the score for your instance. To learn more about ensuring your instances meet hardening requirements, see:

- Instance Security Center
- Adjust instance security settings to increase compliance

Consult the Instance Security Hardening Settings whenever you set or update security-related properties, even if some of the compliance values may not be suitable for your instance. When you are updating these properties, ensure that the instance continues to behave as expected. Consult with the appropriate internal personnel who have the expertise to determine the security impacts.

Other resources

For user reference, the Now Platform maintains extensive configuration capabilities information in the product documentation. You access most of the security content using the links found in Platform security. Also, see the following:

- Available system properties
- General security settings properties
- High Security Settings

Access control (instance security hardening)

Access controls determine whether access to a particular resource should be granted or denied. It only allows access to resources to those users permitted to use them.

Authorization is not equivalent to authentication, as these terms and their definitions are frequently confused.

- Authentication is providing and validating identity.
- Authorization includes execution rules that determine what functionality and data the user (or principal) can access, ensuring the proper allocation of access rights after authentication is successful.

Authorization is a process that comes after a successful authentication. You can configure security properties that designate if, after determining that a user holds valid credentials associated with a well-defined set of roles and privileges, resource authorization occurs.

The following are some security controls that an administrator can configure to restrict unauthorized access to sensitive entities within the Now Platform.

- Access control list rules
- Create an ACL rule
- ServiceNow access control

Basic auth: JSONv2 requests (instance security hardening)

Use the `glide.basicauth.required.jsonv2` property to designate if incoming JSONv2 requests should require basic authorization.

More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.basicauth.required.jsonv2</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To enforce JSONv2 requests authorization.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Medium) This remediation enforces a combination of authentication methods, in the form of basic authentication and system level access control.</td>
</tr>
<tr>
<td></td>
<td>• It performs this authentication while retrieving data from tables/pages in the form of JSON data on the instance.</td>
</tr>
<tr>
<td></td>
<td>• It restricts any guest users who are currently accessing this data.</td>
</tr>
<tr>
<td></td>
<td>• Create an account for a user who needs access to this content, with the necessary access control permissions.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(High) Without appropriate authorization configured on the data source JSON requests, an unauthorized user can access sensitive content/data on the target instance.</td>
</tr>
<tr>
<td>References</td>
<td>Authentication</td>
</tr>
<tr>
<td></td>
<td>Requiring basic authentication for incoming JSONv2 requests</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.

**Basic auth: SOAP requests (instance security hardening)**

Use the `glide.basicauth.required.soap` property to designate if incoming SOAP requests should require basic authorization.

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.basicauth.required.soap</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To enforce soap requests authorization.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Medium) This remediation enforces a combination of authentication methods, in the form of basic authentication and system level access control.</td>
</tr>
<tr>
<td></td>
<td>• It performs this authentication while retrieving data from tables/pages in the form of SOAP data on the instance.</td>
</tr>
<tr>
<td></td>
<td>• It restricts any guest users who are currently accessing this data.</td>
</tr>
<tr>
<td></td>
<td>• Create an account for a user who needs access to this content, with the necessary access control permissions.</td>
</tr>
<tr>
<td></td>
<td>To learn more, see SOAP web service and MID Server authentication credentials and SOAP requests.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(High) Without appropriate authorization configured on the data source SOAP requests, an unauthorized user can access sensitive content/data on the target instance.</td>
</tr>
<tr>
<td>References</td>
<td>Authentication</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.

**Check UI action conditions before execution (instance security hardening)**

Use the `glide.security.strict.actions` property to enable checking of UI actions conditions in forms and lists before they execute. When you set this property to `true`, it adds an extra layer of validation on the table UI actions before they are executed.

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td><code>glide.security.strict.actions</code></td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (<code>/sys_properties_list.do</code>)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To ensure an extra layer of validation on the table UI actions before they are executed.</td>
</tr>
<tr>
<td>Recommended value</td>
<td><code>true</code></td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) This remediation only adds an extra layer of validation to check for UI actions on the target table/page on the instance. As long as the access controls are set appropriately on the customer instance, there should not be an impact here.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) Access request is always checked when transactions happen between two zones. This operation validates any UI actions before the form renders for the end user.</td>
</tr>
<tr>
<td>References</td>
<td>High security plugin</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.
**Contextual Security: Role Management plugin (instance security hardening)**

Activate the Contextual Security: Role Management (`com.glide.role_management`) plugin to enable contextual security, which secures a record/information using create, read, write, and delete functionality.

After it is installed and activated, the dictionary roles (created by simple security manager) are no longer tested. Instead, the Now Platform looks for ACL rules on fields and tables. It secures the data with the help of ACL rules instead of traditional, role-based dictionary rules implemented by simple security manager. Even if you configure the dictionary form and add roles to a dictionary entry, no change in rights occurs.

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plugin ID</td>
<td><code>com.glide.role_management</code></td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Definition &gt; Plugins</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>Unlike the simple security manager, the contextual security manager is aware of the system table hierarchy. You can potentially have different security rules for a field based on where in the hierarchy it appears.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>Active (Plugin activated by default)</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Medium) This remediation enforces functional level of access controls, which would let application determine the access restrictions based on ACL table alone.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(High) Functional level access controls must be enforced from the server side prior to executing CRUD operations, ensuring the appropriate level of access to instance users.</td>
</tr>
<tr>
<td>References</td>
<td>Contextual Security Manager</td>
</tr>
</tbody>
</table>

To learn more about activating a plugin, see [Activate a plugin](#).

**CSV request authorization (instance security hardening)**

Use the `glide.basicauth.required.csv` property to designate if incoming CSV (Comma-Separated Values) requests should require basic authentication.

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td><code>glide.basicauth.required.csv</code></td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To enforce basic authentication on CSV requests.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
</tbody>
</table>
### Functional impact

(Low) This remediation enforces a combination of authentication methods, in the form of basic authentication and system level access control.

- It performs this authentication while retrieving data from tables/pages in the form of CSV data on the instance.
- It restricts any guest users who are currently accessing this data. If applicable, you may need to create a new account for users who need access to this content, with necessary access control permissions.

To learn more, see [Retrieving data from a CSV formatted file](#).

### Security risk

(Medium) Without appropriate authorization configured on the incoming CSV requests, an unauthorized user can get access to sensitive content/data on the target instance.

### References

- [Web service security](#)
- [Add a system property](#)
- [Default deny (instance security hardening)](#)

### Default deny (instance security hardening)

Use the `glide.sm.default_mode` property to control the default behavior of security manager when it finds that existing ACL rules are a part of wildcard table ACL rules.

When the High Security Settings (`com.glide.high_security`) plugin is activated during initial instance installation, it creates this property, and wildcard ACL rules come into existence. To provide role-based access to system tables, these rules control a significant number of ACLs and most common record-based operations:

- Read
- Write
- Create
- Delete

Unless you use the High Security plugin with default deny option enabled, many tables are not protected. The Now Platform uses a default deny security model that prevents non-administrator users from accessing objects unless they meet a matching ACL rule. Using this model, it removes many attack vectors, such as insecure scripts.

### More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td><code>glide.sm.default_mode</code></td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (<code>/sys_properties_list.do</code>)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Attribute Description

**Purpose**
Best security practice would be to restrict an Access to the tables by an unauthorized user.
- If there are no ACL rules in place for tables, this property ensures that at least wildcard ACLs are validated for any CRUD operation performed on the table/field.
- These rules restrict the read, write, create, and delete operations on all tables, unless the user has the admin role or meets the requirements of another table ACL rule.

**Recommended value**
deny

**Functional impact**
(High) If you set this property to *Allow*, the wildcard table ACL rules allow CRUD operations on all tables unless there are specific table ACL rules in place to restrict such operations.

**Security risk**
(High) Non-administrator users can access objects that match the wildcard table ACL rules.

**References**
Default deny property

---

**Double check inbound transactions (instance security hardening)**

Use the `glide.security.strict.updates` property to enable double-checking of security on inbound transactions during form submission. When you set this property to *true*, it adds an extra layer of table validation before a form renders in the browser.

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Property name</strong></td>
<td><code>glide.security.strict.updates</code></td>
</tr>
<tr>
<td><strong>Configuration type</strong></td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td><strong>Configure in Instance Security Center</strong></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>To ensure an added layer of verification of user permissions before presenting the form in the browser.</td>
</tr>
<tr>
<td><strong>Recommended value</strong></td>
<td>true</td>
</tr>
<tr>
<td><strong>Functional impact</strong></td>
<td>(Low) This remediation adds an extra layer of validation to check for user permissions on the target table/page on the instance. As long as the access controls are set appropriately on the customer instance, there should be no impact.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) You should always check access request when transactions happen between two zones. This operation checks for permissions when the form is requested and before form rendering happens.</td>
</tr>
<tr>
<td>References</td>
<td>General security settings properties</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.

**Enable ACLs to control live profile details (instance security hardening)**

Use the `glide.live_profile.details` property to designate whether a user should be able to view all detail fields, such as company name and phone numbers, in a live profile.

Depending on the setting of the `glide.live_profile.details` property, the following occur:

- If the value is set to **Show**, access to the live profile information is granted, regardless of the ACLs created for the user profile.
- If the value is set to **ACL**, access to the live profile information is restricted, as per the ACLs created for the user profile.
- If the value is set to **Hide**, access to the live profile information is restricted, regardless of the ACLs created for the user profile.

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.live_profile.details</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>The purpose is to enable only authorized users to access the details of a Live Profile (such as Company name, Phone numbers)</td>
</tr>
<tr>
<td>Recommended value</td>
<td>ACL</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Medium) If property is not enabled, unauthorized users can access the Live profile details of all other users.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) API requests should always honor table ACLs. Restriction must be applied to prevent unauthorized users accessing details of a Live Profile.</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.

**Enabling AJAXGlideRecord ACL checking (instance security hardening)**

Use the `glide.script.secure.ajaxgliderrecord` property to perform access control rule (ACL) validation when server-side records, such as tables, are accessed using GlideAjax APIs within a client script.

From client scripts, it is possible to query arbitrary data from the server using the AJAXGlideRecord (GlideAjax - Client) API, by using a syntax such as a server-side glide record. It is a powerful and useful tool in many deployments.
If you choose to apply, Access Control Lists (ACL) to GlideAjax API calls, you can only query data to which the currently connected user has access. For example, if an ESS user who has no rights to read the cmn_location table is logged in, any GlideAjax API call to that table would fail.

If the Now Platform is running without GlideAjax ACL call checking, an API can return information that the currently logged in user could not otherwise access.

More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.script.secure.ajaxgliderecord</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>Ensure security ACLs are checked and validated even when the records are accessed through Client Side APIs.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(High) This remediation enforces the ACL relationship with server-side records when the requests are made using the AJAXGlideRecord API calls. If the ACL configuration is not properly configured, then there is potential impact. For more details on its impact, and how to identify it, see Refer to the Audit and review client-side GlideRecord (AJAXGlideRecord) transactions [KB0550828] article in the HI Knowledge Base.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(High) Through client scripts, it is possible to query arbitrary data from the server through the GlideAjax API. Server-side resources can be accessed without proper authorization, so using ACL validation helps the application validate the request based on the configured authorization.</td>
</tr>
<tr>
<td>Workaround</td>
<td>Ensure that proper ACLs are created for script includes, processors, and other entities used by a GlideAjax (AJAXGlideRecord) API so that it executes under proper authorization. Implement methods like canRead(), canWrite(), canCreate(), and canDelete() to perform user authorization before accessing table records using GlideRecord. Another method is to use GlideRecordSecure. The class is inherited from the GlideRecord Server that performs the same functions as GlideRecord, and also enforces ACLs.</td>
</tr>
<tr>
<td>References</td>
<td>Apply ACLs to AJAXGlideRecord (client-side Glide record)</td>
</tr>
</tbody>
</table>

This property belongs to the same family of properties that secure and restrict execution of scripts originating from the client:

- glide.script.use.sandbox: See Client generated scripts sandbox.
- glide.script.allow.ajaxevaluate: See Enable AJAXEvaluate.

To learn more about adding or creating a system property, see Add a system property.
Excel request authorization (instance security hardening)

Use the `glide.basicauth.required.excel` property to designate if incoming Excel requests should require basic authentication.

More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.basicauth.required.excel</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To enforce basic authentication on Excel requests.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) This remediation enforces a combination of authentication methods, in the form of basic authentication and system level access control.</td>
</tr>
<tr>
<td></td>
<td>• It performs this authentication while retrieving data from tables/pages in the form of Excel data on the instance.</td>
</tr>
<tr>
<td></td>
<td>• It restricts any guest users who are currently accessing this data. If applicable, you may need to create a new account for users who need access to this content, with necessary access control permissions.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) Without appropriate authorization configured on the incoming Excel requests, an unauthorized user can get access to sensitive content/data on the target instance.</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.

Explicit Role plugin (instance security hardening)

Activate the Explicit Role (com.glide.explicit_roles) plugin to provide the instance with the new snc_internal and snc_external roles for B2B and B2C applications, preventing external users from accessing internal data. Enterprise users (employees) must have the internal role while non-enterprise users (non-employees) must have the external role.

When you install the explicit role plugin:

- It assigns all existing users with the new snc_internal role. It also assigns all tables without any role with the snc_internal role.
- When you create a user or table after activating the Explicit Role plugin, the Now Platform assigns the user or table with the snc_internal role.
- The Now Platform prevents the users with the snc_external role from accessing any table that is not explicitly assigned with the snc_external role.
- Any table with the public role are accessible by both internal or external users.

Role summary

snc_internal
This role is assigned to all internal users (employee or internal to an organization). Any new user that gets added also get this role during their first login/impersonation, provided the user doesn't have the snc_external role already assigned. All the existing ACLs without a role are patched with the 'snc_internal' role. For new ACLs, the Now Platform automatically adds this role if the ACL is saved without any role.

**snc_external**

This role indicates that the user is external to your organization and should not have any access to resources unless:

- You explicitly allow access through ACLs for the snc_external role, or
- You explicitly grant them additional roles.

By default, users with the snc_external role are unable to access non-record type resources as well, such as processors and UI pages.

**public**

Any entities with public role assigned to it are accessible by both snc_internal and snc_external users.

When using Explicit Role plugin:

1. Review and validate that any table with the public role doesn't contain any sensitive record to the external users, including unauthenticated public users.

2. If the table with the public role contains sensitive data, and you want to restrict the sensitive records from external users, either:
   - Remove the public role from the table or
   - Add additional scripted ACL to the table.

3. Review and validate that all endpoints, such as the Scripted REST APIs, use the **GlideRecordSecure** or explicitly check roles using `canRead()`, `canWrite()`, `canUpdate()`, and `canDelete()`.

### More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Plugin Name</strong></td>
<td>com.glide.explicit_roles</td>
</tr>
<tr>
<td><strong>Configuration type</strong></td>
<td>System Definition &gt; Plugin</td>
</tr>
<tr>
<td><strong>Configure in Instance Security Center</strong></td>
<td>No</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>To prevent external users from accessing internal data.</td>
</tr>
<tr>
<td><strong>Recommended value</strong></td>
<td>Active</td>
</tr>
<tr>
<td><strong>Functional impact</strong></td>
<td>(Low) No significant impact as the plugin automatically assigns the snc_internal role to the table so the existing internal users still have the necessary access.</td>
</tr>
<tr>
<td><strong>Security risk</strong></td>
<td>(High) External Users (Non-employees) can access to many sensitive tables in the Now Platform that do not have any roles assigned to it. They are meant to be accessible by internal users (Employees) only.</td>
</tr>
<tr>
<td><strong>References</strong></td>
<td>Explicit Roles</td>
</tr>
</tbody>
</table>
Steps to configure

When creating feature or application with the explicit roles:

1. Create a role that inherits the snc_external role for your new feature or application.
2. When creating an external user, remove the snc_internal role and add the newly created role that inherits the snc_external role.
3. When adding the new role that inherits the snc_external role to the existing table, review and validate that the table doesn't contain any sensitive record.
4. When creating a table, validate that the table is accessible only by authorized internal and external user roles.
5. When creating endpoints such as the Scripted REST API, use GlideRecordSecure or explicitly check roles using `canRead()`, `canWrite()`, `canUpdate()`, and `canDelete()`.

When creating a table with the public role, make sure that the table doesn't contain any sensitive record to the external users including unauthenticated public users.

Import request authorization (instance security hardening)

Use the `glide.basicauth.required.importprocessor` property to designate if incoming import requests should require basic authentication.

More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.basicauth.required.importprocessor</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To enforce basic authentication on import requests.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) This remediation enforces a combination of authentication methods, in the form of basic authentication and system level access control.</td>
</tr>
<tr>
<td></td>
<td>• It performs this authentication while importing data sources into the instance tables/pages.</td>
</tr>
<tr>
<td></td>
<td>• It restricts any guest users who are currently accessing this data. If applicable, you may need to create a new account for users who need access to this content, with necessary access control permissions.</td>
</tr>
<tr>
<td></td>
<td>To learn more, see Retrieving data from a CSV formatted file.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) Without appropriate authorization configured on the datasource import requests, an unauthorized user can get access to sensitive content/data on the target instance.</td>
</tr>
<tr>
<td>References</td>
<td>SOAP web services security SOAP web service</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.
PDF request authorization (instance security hardening)

Use the \texttt{glide.basicauth.required.pdf} property to designate if incoming PDF requests should require basic authentication.

More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>\texttt{glide.basicauth.required.pdf}</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To enforce basic authentication on PDF requests.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
</tbody>
</table>
| Functional impact             | (Low) This remediation enforces a combination of authentication methods, in the form of basic authentication and system level access control.  
• It performs this authentication while retrieving data from tables/pages in the form of PDF data on the instance.  
• It restricts any guest users who are currently accessing this data.  
If applicable, you may need to create a new account for users who need access to this content, with necessary access control permissions.  
To learn more, see Web service import sets. |
| Security risk                 | (Medium) Without appropriate authorization configured on the incoming PDF requests, an unauthorized user can get access to sensitive content/data on the target instance. |

To learn more about adding or creating a system property, see Add a system property.

Performance monitoring (ACL) (instance security hardening)

Use the \texttt{glide.security.diag\_txns\_acl} property to control stats.do, threads.do, thread\_pool\_stats, and replication.do access from an unauthenticated connection.

When you set this property to \texttt{true}, the \texttt{glide.security.diag\_txns\_acl} property only allows access to the following by the administrator account:

• https://<instancename>.servicenow.com/stats.do
• https://<instancename>.servicenow.com/threads.do
• https://<instancename>.servicenow.com/replication.do
• https://<instancename>.servicenow.com/thread\_pool\_stats.do

Without enabling this setting, it is still possible to access these resources from an unauthenticated connection.
More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.security.diag_txns_acl</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>Restrict the access to configuration pages to administrator account only</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) This remediation enforces only administrator account to get access to the application sensitive data for logging and troubleshooting purposes.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Low) Sensitive data such as server details, threads, and processes executed on the server should never be visible or accessible to the end user without appropriate privileges.</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.

Performance monitoring IP restriction (instance security hardening)

Use the **glide.custom.ip.authenticate.allow** property to enable only a specified comma-separated list or a range of IP addresses access to stats.do, threads.do, and replication.do pages. If this property is not enabled, it is possible to access those types of pages from any IP address.

**Note:** Based on some recent changes, IP Address Access Control must be used for all IP restriction. Refer to the Steps to Configure section in Restrict access to specific IP ranges.

More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.custom.ip.authenticate.allow</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>No</td>
</tr>
<tr>
<td>Purpose</td>
<td>Restrict the access only to configuration pages to the IP addresses in the inclusion list.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>Comma-separated list of IP address.</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) Sensitive information pages can be accessed even from an untrusted IP address.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Low) Unnecessary exposure to the target instance on the internet should be restricted with the help of IP access controls functionality.</td>
</tr>
<tr>
<td>Reference</td>
<td>Available system properties</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.
Privacy on client-callable script includes (instance security hardening)

By default, client-callable script includes that do not explicitly set visibility, are public. If needed, add the `glide.script.ccsi.ispublic` property to enable privacy control over all client-callable script includes accessed by public pages.

When you add this property, you must set its value to `false`, which designates that all client-callable script includes are private, and changes their visibility in public pages.

Note: You cannot add the property with a value of `true`, or change its value from `false` to `true`. If you attempt to do so, an error message appears.

If needed, you can change the privacy setting for an individual client-callable script include by adding the `isPublic()` function.

- The `isPublic()` setting takes precedence over the `glide.script.ccsi.ispublic` property.
- For example, if you set `isPublic()` to `true` in an individual script, it makes it public, which overrides the `glide.script.ccsi.ispublic` property that makes all other client-callable script includes private.

More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td><code>glide.script.ccsi.ispublic</code></td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>Making client-callable script includes private means that guests who access public pages can't access the client-callable script include. A non-logged-in user can't execute a private script.</td>
</tr>
<tr>
<td>Recommended value</td>
<td><code>false</code></td>
</tr>
<tr>
<td>Functional impact</td>
<td>(High) If the client-callable script includes are designated as public (that is, this property is missing), then unauthenticated users can execute client scripts. Add the property restricts the execution of scripts by a non-logged-in user.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(High) If you do not add this property, client-side script includes circumvent ACLs, which may result in unintended public functionality. If the client script provides confidential information, it could have an adverse potential security risk.</td>
</tr>
<tr>
<td>Workaround</td>
<td>Setting the <code>glide.script.ccsi.ispublic</code> property to <code>false</code> makes all client-callable script includes private. You can change the privacy setting for an individual client-callable script include by adding the <code>isPublic()</code> function. The <code>isPublic</code> function takes precedence over the <code>glide.script.ccsi.ispublic</code> property. Add the following syntax to the script include: <code>isPublic:function(){return[true/false];}</code>,</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.
Restrict access to specific IP ranges (instance security hardening)

Use the `com.snc.ipauthenticator` property to restrict access to specific IP ranges. Unless public access is intended for the instance, administrators should limit access to their assigned IP net blocks.

**Prerequisites**

Before setting this property, you must activate the IP Range Based Authentication `com.snc.ipauthenticator` plugin. To learn more, see IP range based authentication and in the Steps to configure section (below).

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plugin Name</td>
<td>com.snc.ipauthenticator</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Security &gt; IP Address Access Control</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To add the range of IP address that can or can't access the instance to the trusted and untrusted domain lists.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>Active</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) Customer-denied IP ranges are used for this remediation item. No impact as customer defines the target list.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Low) Unnecessary exposure to the target instance on the internet should be restricted with the help of IP access controls functionality.</td>
</tr>
<tr>
<td>References</td>
<td>IP range based authentication</td>
</tr>
</tbody>
</table>

**Steps to configure**

1. Ensure that the `com.snc.ipauthenticator` plugin is active.

2. Navigate to **System Security > IP Address Access Control**.

3. Click **New** to create an exclusion list (Deny) or an inclusion list (Allow) of IP addresses.
4. Click Submit.

![Image of a web interface for setting permissions]

**RSS request authorization (instance security hardening)**

Use the `glide.basicauth.required.rss` property to designate if incoming RSS requests should require basic authentication.

### More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td><code>glide.basicauth.required.rss</code></td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To enforce basic authentication on RSS requests.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) This remediation enforces a combination of authentication methods, in the form of basic authentication and system level access control.</td>
</tr>
<tr>
<td></td>
<td>• It performs this authentication while processing RSS requests on the instance.</td>
</tr>
<tr>
<td></td>
<td>• It restricts any guest users who are currently accessing this data. If applicable, you may need to create a new account for users who need access to this content, with necessary access control permissions.</td>
</tr>
<tr>
<td></td>
<td>To learn more, see RSS feed generator.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) Without appropriate authorization configured on the incoming RSS requests, an unauthorized user can get access to sensitive content/data on the target instance.</td>
</tr>
<tr>
<td>References</td>
<td>RSS basic authentication</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see [Add a system property](#).
SAML 2.0 web browser SSO profile (instance security hardening)

The `com.snc.integration.sso.saml20.update1` plugin ensures that the status of the SAML 2.0 Single Sign-On plugin is active.

Security Assertion Markup Language (SAML) is an XML-based standard for exchanging authentication and authorization data between security domains. SAML exchanges security information between an identity provider (a producer of assertions) and a Service Provider (a consumer of assertions).

The `com.snc.integration.sso.saml20.update1` plugin is a required plugin, but you do not need to manually activate it. The `sso.multi.installer` installs all required SAML-related plugins, and also contains saml2 implementation scripts that provide options for response validation. To learn more, see the topics in References in More Information.

More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plugin Name</td>
<td><code>com.snc.integration.sso.saml20.update1</code> (new)</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Definition &gt; Plugins</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To prevent against cross-site scripting attacks.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>Active</td>
</tr>
<tr>
<td>Role required</td>
<td>Your administrator can't activate the plugin. Request that person with elevated security privileges activate it on the instance.</td>
</tr>
<tr>
<td>References</td>
<td>Authentication with SAMLAuthentication with SAMLIntegrationUpgrading SAML 2.0 integration</td>
</tr>
</tbody>
</table>

To learn more about activating a plugin, see [Activate a plugin](#).

Script request authorization (instance security hardening)

Use the `glide.basicauth.required.scriptedprocessor` property to designate if incoming script requests should require basic authentication.

More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td><code>glide.basicauth.required.scriptedprocessor</code></td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To enforce basic authentication on scripts requests.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Medium) This remediation enforces the authentication in the form of Basic authorization.</td>
</tr>
<tr>
<td></td>
<td>• It performs this authentication while processing script requests on the instance.</td>
</tr>
<tr>
<td></td>
<td>• It restricts any guest users who are currently accessing this data. If applicable, you may need to create a new account for users who need access to this content, with necessary access control permissions.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(High) Without appropriate authorization configured on the incoming script requests, an unauthorized user access sensitive content/data on the target instance.</td>
</tr>
<tr>
<td>References</td>
<td>Authentication</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.

**Security jump start (ACL rules) (instance security hardening)**

Activate the Security Jump Start (ACL Rules) (**com.snc.system_security**) plugin to create several important ACLs that validate the Access Controls on some of the key system tables within the Now Platform.

These rules provide a jump-start on securing many system tables, making it easier for an organization to get an instance into production. The Security Jump Start (ACL Rules) plugin is installed automatically on all new instances.

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plugin ID</td>
<td>com.snc.system_security</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Definition &gt; Plugins</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>Activate the Security Jump Start (ACL Rules) plugin to achieve proper security compliance.</td>
</tr>
<tr>
<td></td>
<td>It provides some basic ACLs that secure system tables in the first place instead of creating manually for each system table that comes with default provisioning of an instance. These ACLs are helpful when the newly created instance must quickly move into production.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>Active</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Medium) There is significant functional impact if this plugin is installed without auditing of the existing ACLs on the instance. Customer outreach and definitions are required before the remediation can occur.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(High) Access control should be enforced to lock down the unintended access to the instance. ACL jumpstart rules were created to provide a starting point on securing many system tables to make it easier for an organization to quickly get into production.</td>
</tr>
</tbody>
</table>
### Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>References</td>
<td>Security jump start - ACL rules</td>
</tr>
</tbody>
</table>

### Steps to configure

If this plugin is not activated on your instance, contact ServiceNow Support. Activating the plugin at this point might modify security access to tables already in use in a production environment. If an administrator is interested in the new ACL rules the plugin provides, you can manually create one or more of them in an existing instance if needed. This list of ACLs may be used as a guideline in that case.

To learn more about activating a plugin, see [Activate a plugin](#).

### SNC Access Control plugin (instance security hardening)

Activate the SNC Access Control ([com.snc.snc_access_control](#)) plugin to control access to your instances by Customer Service and Support personnel.

The default configuration for the Now Platform enables Customer Service and Support to access instances through an internal process that creates short-term support credentials. Although all access is audited, some customers prefer to control this access.

This plugin enables the Customer Administrator to prohibit Customer Service and Support employees from accessing the instance. This decision does have an impact on support SLAs because you must enable Now Platform access before support activities can begin. To learn more, see [ServiceNow access control](#).

### More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plugin Name</td>
<td>com.snc.snc_access_control</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Definition &gt; Plugins</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>Prohibits Customer Service and Support employees from accessing the instance</td>
</tr>
<tr>
<td>Recommended value</td>
<td>Active</td>
</tr>
<tr>
<td>Role required</td>
<td>The customer administrator can't activate this plugin. It must be explicitly requested because it requires elevated privileges to activate the plugin.</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) If this plugin is inactive, all Customer Service and Support employees can access the customer's instance. Enabling the plugin enables the customer to restrict access to authorized Customer Service and Support employees only.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Low) Unnecessary exposure of instance access to wider group of people</td>
</tr>
<tr>
<td>References</td>
<td>ServiceNow access control</td>
</tr>
</tbody>
</table>
Steps to configure

1. To request the plugin, follow the steps in Request ServiceNow access control. Customers must request the SNC Access Control plugin (com.snc.snc_access_control) from HI.

2. To enable SNC access control, follow the steps in Configure ServiceNow access control. Configure an access control record to specify one or more Customer Service and Support employees that have permission to log in your instance.

SOAP content type checking (instance security hardening)

Use the `glide.soap.require_content_type_xml` property to enable validation of a content type as text/xml and protect against invalid SOAP requests.

- When set to `true`, the Now Platform validates the content type as text/xml and protects against invalid SOAP requests.
- If set to `false`, any content-type value is allowed.

More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td><code>glide.soap.require_content_type_xml</code></td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>Protect against invalid SOAP requests</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) This remediation enables validation of SOAP content type for all the inbound SOAP requests.</td>
</tr>
<tr>
<td></td>
<td>• If you are using a content type other than text/xml for inbound requests, it may cause potential failure of SOAP transactions.</td>
</tr>
<tr>
<td></td>
<td>• If you are not using the correct MIME type, it could disrupt third-party integrations.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(High) When accepting inbound SOAP requests, the appropriate validation is performed to ensure that the relevant content type is being defined as a part of the request. It restricts the invalid SOAP responses that can be viewed as a security risk.</td>
</tr>
<tr>
<td>Reference</td>
<td>Content types</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.
**Strict IP restriction (instance security hardening)**

Use the `glide.ip.authenticate.strict` property to enable a strict set of IP addresses, such as DC and secure VPN, to access this instance.

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.ip.authenticate.strict</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>Allows ServiceNow employees to access the instance only through secured set of IP ranges</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) If this property is not enabled, ServiceNow employees can access the customer’s instance through all the IP ranges. Enabling the property restricts access to a secure set of IP ranges (Secure VPN, DC).</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Low) Unnecessary exposure of instance access to wider group of people.</td>
</tr>
<tr>
<td>Reference</td>
<td>IP range based authentication</td>
</tr>
</tbody>
</table>

**Note:** If you set this property to true, the Now Platform uses a more restrictive `glide.ip.authenticate.allow.secured` property instead of the Performance Monitoring IP restriction `glide.ip.authenticate.allow.secured` property for a set of IP ranges that can access the instance.

To learn more about adding or creating a system property, see [Add a system property](#).

**Unload request authorization (instance security hardening)**

Use the `glide.basicauth.required.unl` (useUnloadFormat) property to designate if incoming unload requests should require basic authentication.

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.basicauth.required.unl</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To enforce basic authentication on unload requests.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
</tbody>
</table>
**ServiceNow**  
**DocVersion**  
**Now Platform administration**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional impact</td>
<td>(Medium) This remediation enforces a combination of authentication methods, in the form of basic authentication and system level access control. It performs this authentication while retrieving data from tables/pages in the form of unload data on the instance.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(High) Without appropriate authorization configured on the datasource unload requests, an unauthorized user can get access to sensitive content/data on the target instance.</td>
</tr>
<tr>
<td>References</td>
<td>Authentication</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see [Add a system property](#).

### WSDL request authorization (instance security hardening)

Use the `glide.basicauth.required.wsd`l property to designate if incoming WSDL (Web Services Description Language) requests should require basic authentication.

**Note:** If you choose not to require basic authentication for incoming WSDL requests, you must modify Access Control (ACL) rules to enable guest users to access the WSDL content.

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td><code>glide.basicauth.required.wsd</code></td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To enforce basic authentication on WSDL requests.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
</tbody>
</table>
| Functional impact         | (Low) This remediation enforces a combination of authentication methods, in the form of basic authentication and system level access control.  
  • It performs this authentication while retrieving data from tables/pages in the form of WSDL data on the instance.  
  • It restricts any guest users who are currently accessing this data. If applicable, you may need to create a new account for users who need access to this content, with necessary access control permissions. |
| Security risk             | (Medium) Without appropriate authorization configured on the WSDL web services, an unauthorized user can get access to sensitive WSDL content/data on the target instance. |
| References                | Web service security                                                                                                                             |

To learn more about adding or creating a system property, see [Add a system property](#).
XML request authorization (instance security hardening)

Use the glide.basicauth.required.xml property to designate if incoming XML requests should require basic authentication.

More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.basicauth.required.xml</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To enforce basic authentication on XML requests.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) This remediation enforces a combination of authentication methods, in the form of basic authentication and system level access control.</td>
</tr>
<tr>
<td></td>
<td>• It performs this authentication while retrieving data from tables/pages in the form of XML data on the instance.</td>
</tr>
<tr>
<td></td>
<td>• It restricts any guest users who are currently accessing this data. If applicable, you may need to create a new account for users who need access to this content, with necessary access control permissions.</td>
</tr>
<tr>
<td></td>
<td>To learn more, see XML parser step.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) Without appropriate authorization configured on the incoming XML requests, an unauthorized user can get access to sensitive content/data on the target instance.</td>
</tr>
<tr>
<td>References</td>
<td>Authentication</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.

XSD request authorization (instance security hardening)

Use the glide.basicauth.required.xsd property to designate if incoming XSD (XML Schema Definition) requests should require basic authentication.

More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.basicauth.required.xsd</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To enforce basic authentication on XSD requests.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Functional impact    | (Low) This remediation enforces a combination of authentication methods, in the form of basic authentication and system level access control.  
• It performs this authentication while retrieving data from tables/pages in the form of XSD data on the instance.  
• It restricts any guest users who are currently accessing this data. If applicable, you may need to create a new account for users who need access to this content, with necessary access control permissions.  
To learn more, see Non-interactive sessions. |
| Security risk        | (Medium) Without appropriate authorization configured on the incoming XSD requests, an unauthorized user can get access to sensitive content/data on the target instance.                                                                 |
| References           | Authentication                                                                                                                                                                                                |

To learn more about adding or creating a system property, see Add a system property.

**Attachments (instance security hardening)**

Many Now Platform business processes allow for the upload of data/information. It regularly checks the validity and security of text, but accepting these files can introduce even more risk.

To reduce the risk, you should validate for malicious files so that the Now Platform can correctly protect against attackers who send these files. You handle these files by including business logic that scans files during the upload process and rejects those files perceived as malicious.

**Internal References**

- Administering attachments
- Configure attachment system properties

**Downloadable MIME types (instance security hardening)**

Use the glide.ui.attachment.download_mime_types property to specify a list of comma-separated attachment MIME types that should be downloaded but not render inline in the browser.

To view a listing of existing MIME types, type /sys_attachment_icon_rule_list.do. You can enable any one of these MIME types to meet the security compliance requirements within the Now Platform.

**Note:** If you set the Force Download MIME Types property to true, it overrides the Downloadable MIME types property, which is a comma-delimited listing of downloadable MIME types. To learn more, see Force download MIME types.
### Attribute Description

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.ui.attachment.download_mime_types</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To restrict the file types from being rendered in the browser to avoid any hidden malicious script execution.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>Some defined file types, for example, text/html, text/csv.</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) This remediation enforces performance of validation checks before performing an action when you click an attachment in a Now Platform application. There is no potential impact, but the user experience is altered.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) Client-side scripting attack vectors come in different flavors and MIME type attachment abuse is no exception. Attackers can abuse MIME types and place unintended script content in the attachment on the victim's side to capture sensitive information. In the current context, populate the property with a list of comma-separated attachment mime types that should not render inline in the browser. Example: text/html</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see [Add a system property](#).

### Enable blacklist for attachments (instance security hardening)

Use the `glide.security.attachment_type.use_blacklist` property to designate if the Now Platform should validate the attachment against a specified exclusion list.

**Note:** Set this property before setting the `glide.attachment.blacklisted.extensions` and `glide.attachment.blacklisted.types` properties. To learn more, see [Specify excluded attachment extensions](#) (instance security hardening) and [Specify excluded attachment file types](#) (instance security hardening).

### More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.security.attachment_type.use_blacklist</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>Restrict upload (Insert/Write/Update) operation of attachments with questionable file extensions and file types, such as exe, dll, jar, text/html.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) No functionality impact unless there is an attempt to upload any file extensions or file types that are specified under exclusion listed properties <em>(glide.attachment.blacklisted.extensions and glide.attachment.blacklisted.types)</em></td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) A malicious user can upload malware infected attachment with common executable file extensions and/or types.</td>
</tr>
<tr>
<td>Workaround</td>
<td>Properties are available in the base system that address the same issue with inclusion lists instead of exclusion lists. To learn more, see:</td>
</tr>
<tr>
<td></td>
<td>• Restrict file extensions (instance security hardening)</td>
</tr>
<tr>
<td></td>
<td>• Upload MIME type restriction (instance security hardening)</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.

**Enable file download restrictions (instance security hardening)**

Use the *glide.ui.strict_customer_uploaded_static_content* property to enable restrictions on the file types that can be downloaded when they have been uploaded using the Upload File functionality.

You use this property with the *glide.ui.strict_customer_uploaded_content_types* property, which creates a comma-delimited list of restricted downloadable file types. To learn more, see Downloadable file types.

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.ui.strict_customer_uploaded_static_content</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>No</td>
</tr>
<tr>
<td>Purpose</td>
<td>To ensure that safe file types are permitted to be downloaded from the application.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) This remediation enforces restriction of file downloads based on the values specified in the <em>glide.ui.strict_customer_uploaded_content_types</em> property. To learn more, see Downloadable file types.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) File download restrictions should be applied to any untrusted user input sources.</td>
</tr>
</tbody>
</table>

**Enforce strict user image upload (instance security hardening)**

Use the *glide.security.strict.user_image_upload* property to enable Access Control for the upload/update of a profile picture when performed on a user record.

This setting opens the possibility of an unauthorized user uploading an image to another user's profile.

- When you set this property to true, the table ACLs are enforced when uploading photos, only allowing authorized users to upload an image.
• When you set it to false, ACLs are not enforced on image uploads to the Photo field.

More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.security.strict.user_image_upload</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To restrict uploading of user image only to authorized users.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) No functionality impact as authorized users are still able to upload images to their user profile.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) When you set this property to false, an authenticated user could upload an image to another user's account without authorization.</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.

Force Download MIME types (Instance security hardening)

Use the glide.ui.attachment.force_download_all_mime_types property to force the download of all MIME type attachments.

**Note:** If you set the Force Download MIME Types property to true, it overrides the Downloadable MIME types property, which is a comma-delimited listing of downloadable MIME types. To learn more, see Downloadable MIME types.

More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.ui.attachment.force_download_all_mime_types</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>No</td>
</tr>
<tr>
<td>Purpose</td>
<td>To enforce download of all attachments, instead of executing in the browser.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Medium) This remediation enforces the download of all attachments. No functionality impact, but it results in altered user experience.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(High) To reduce the client-side scripting attacks, file attachments should be force downloaded as opposed to being rendered in the browser context.</td>
</tr>
</tbody>
</table>

References

Available system properties
To learn more about adding or creating a system property, see Add a system property.

**Restrict file extensions (instance security hardening)**

Use the `glide.attachment.extensions` property to create a comma-delimited list of restricted downloadable file extension types. The specified files extension types are the only ones that can be uploaded as attachments. Using this property improves security by preventing users from uploading harmful files, such as viruses, as attachments.

This functionality can also prevent the use of incompatible file types. For example, some browsers do not support icons in a .png format. This property doesn't restrict files based on the actual file type, but only based on the extension. If no extensions are specified, then all extensions are allowed. However, if any extensions are specified, all unlisted extensions are restricted.

**Note:** Set this property before setting the `glide.security.file.mime_type.validation` property. Only those extensions specified within this property are checked for MIME type during upload. To learn more, see Upload MIME type restriction.

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.attachment.extensions</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To only enable acceptable file extensions to be uploaded during file attachment. It blocks an attempt to upload potentially malicious extensions.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>Some defined file extensions, such doc, docx, pdf, xls, xlsx</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Medium) This remediation restricts all the file extensions except the ones in the inclusion list. No functionality impact unless there is an attempt to upload any file other than extensions acceptable by organization.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) As MIME type verification depends on this property, it is recommended to mitigate against the vulnerabilities related to malicious file upload.</td>
</tr>
</tbody>
</table>

**Steps to configure**

1. Navigate to `/sys_properties_list.do`.
2. Search for the `glide.attachment.extensions` property.
3. Specify the acceptable downloadable file extensions in a comma-separated list as shown, then click **Update**.

![System Property glide.attachment.extensions](image)

<table>
<thead>
<tr>
<th>Name</th>
<th>glide.attachment.extensions</th>
<th>Application</th>
<th>Global</th>
<th>Update</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>List of file extensions (comma-separated) that can be attached to documents via the attachment dialog. Extensions should not include the dot (.) e.g., xlx,xls,doc,docx. Leave blank to allow all extensions.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Choices</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>string</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Value</td>
<td>doc,docx,xls,xlsx,pdf,jpeg,jpg,png,ico</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ignore cache</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Private</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Read roles</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Write roles</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Restrict unauthenticated access to attachments (instance security hardening)

Use the `glide.image_provider.security_enabled` property to control the security settings for images. If set to `true`, images are visible only to authenticated and authorized users. If set to `false`, images are visible to anyone with a URL to the attachment.

### More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.image_provider.security_enabled</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To prevent unauthenticated access of attachment when rendered using the .iix format.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) No significant impact on the functionality. User experience might be affected a bit because the user who formerly directly accessed .iix must go through authentication.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(High) Restriction must be applied for unauthenticated users as some attachment might contain sensitive information.</td>
</tr>
<tr>
<td>References</td>
<td>Administering attachments</td>
</tr>
<tr>
<td></td>
<td>Available system properties</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see [Add a system property](#).

Specify excluded attachment extensions (instance security hardening)

When you enable exclusion list validation in the Now Platform, use the `glide.attachment.blacklisted.extensions` property to create a comma-delimited list of restricted uploadable file extension types. Uploading of the specified file extension types is restricted.

### Prerequisites

Before setting this property, set the `glide.security.attachment_type.use_blacklist` property to true. To learn more, see [Enable blacklist for attachments](#).

### More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.attachment.blacklisted.extensions</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>Restrict upload (Insert/Write/Update) operation of attachments with questionable file extensions.</td>
</tr>
<tr>
<td>Type</td>
<td>String</td>
</tr>
</tbody>
</table>
To learn more about adding or creating a system property, see Add a system property.

Specify excluded attachment file types (instance security hardening)

When the exclusion list validation is enabled in the Now Platform, use the `glide.attachment.blacklisted.types` property to create a comma-delimited list of restricted uploadable file types. Uploading of the specified file types is restricted.

Prerequisites

Before setting this property, set the `glide.security.attachment_type.use_blacklist` property to true. To learn more, see Enable blacklist for attachments.

More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.attachment.blacklisted.types</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>Restrict upload (Insert/Write/Update) operation of attachments with questionable file types. Example: text/html.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>Some Defined File Types (For example: text/html,text/csv).</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) No functionality impact unless there is an attempt to upload any file type that is specified under this property.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) A malicious user can upload malware infected attachment with common executable file types.</td>
</tr>
</tbody>
</table>
| Workaround         | Properties are available in base system functionality that address the same issue with inclusion listing rather than with exclusion listing. To learn more, see:  
                       • Restrict file extensions  
                       • Upload MIME type restriction |
To learn more about adding or creating a system property, see Add a system property.

**Downloadable file types (instance security hardening)**

Use the glide.ui.strict_customer_uploaded_content_types property to create a comma-delimited list of restricted downloadable file types. The specified files types are the only ones that can be downloaded as static content from an instance.

### More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.ui.strict_customer_uploaded_content_types</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To ensure that only file types in inclusion lists are allowed to be downloaded.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>User Specified (Common: doc, docx, xls, xlsx, pdf, and the like)</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Medium) Only files that are in inclusion lists can be downloaded which might affect the organization policy. The comma-separated inclusion list must be modified to comply with organization's policy for acceptable downloadable file types.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Low) File download restrictions should be applied to any untrusted user input sources.</td>
</tr>
<tr>
<td>References</td>
<td>General security settings properties</td>
</tr>
<tr>
<td></td>
<td>Content types</td>
</tr>
</tbody>
</table>

### Steps to configure

1. Navigate to /sys_properties_list.do.
2. Search for the glide.ui.strict_customer_uploaded_content_types property.
3. Specify the acceptable downloadable file types in a comma-separated list as shown, then click **Update**.

![Upload MIME type restriction (instance security hardening)](image)

**Upload MIME type restriction (instance security hardening)**

Use the `glide.security.file.mime_type.validation` property to activate MIME type checking for uploads. You can enable (set the property to **true**) or disable (set it to **false**) MIME type validation for file attachments.

**Prerequisites**

Before setting this property, set the `glide.attachment.extensions` property. Only those extensions specified in `glide.attachment.extensions` are checked for MIME type during upload. To learn more, see **Restrict file extensions**.

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td><code>glide.security.file.mime_type.validation</code></td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To enforce checking of MIME type / magic bytes during file uploads.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Medium) This remediation enables MIME type verification on the attachments to the application. No functionality impact, unless there is a malicious intent in uploading the files as this validation is merely checking for mis-sync between the MIME type and the data.</td>
</tr>
</tbody>
</table>
### Email security (instance security hardening)

This section contains security controls an administrator can configure to ensure that proper security policies are in place for all inbound emails.

**Convert inbound email HTML (instance security hardening)**

Use the `glide.email.inbound.convert_html_inline_attachment_references` property to specify whether to convert inbound email HTML so email images appear in the email HTML body preview.

In the Now Platform, broken cid (content ID) links appear in place of images received when you set this property to false. The format in which the email image appears depends on the property setting at the time the email is received, not the current property setting.

Whatever ‘malicious’ content is received in the attachment is not referenced in the HTML in the email. The attachment itself is stored in the `sys_attachment` table.

**Prerequisites**

Before setting this property, set the `glide.email.read.active` property to true. To learn more, see [Enable using your own POP3 server](#).

### More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td><code>glide.email.inbound.convert_html_inline_attachment_references</code></td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To restrict image rendering in HTML body preview.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>false</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Medium) Once this property is configured, user are not able to see the image preview in the email body.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) If the property is not enabled, an attacker might send malicious image containing malware.</td>
</tr>
<tr>
<td>References</td>
<td>Email properties</td>
</tr>
<tr>
<td></td>
<td>Inbound mail configuration</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see [Add a system property](#).
Email spam scoring and filtering (instance security hardening)

Install the Email Filter (`com.glide.email_filter`) plugin to install email filtering within the instance. This filtering identifies existing headers, which enables you to decide what to do with the email based on the associated header. Every message sent through Now Platform email servers is assessed for the likelihood of being spam.

**Note:** If an instance uses a private email server, this topic is not applicable. For more information, see Email Spam Scoring and Filtering.

**Prerequisites**

Before setting this property:

- Set the `glide.email.read.active` property to true. To learn more, see Enable using your own POP3 server.
- Create a comma-separated list, in the `glide.pop3.ignore_headers` property, of email headers that cause the instance to ignore an email message. To learn more, see Available system properties.

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plugin Name</td>
<td><code>com.glide.email_filter</code></td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Definition &gt; Plugins</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To enforce filtering to avoid spamming of emails.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>Active</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) Email is never filtered, blocked, or quarantined from the instance as part of spam scoring. It is only scored and then sent on to the instance. All filtering is done within the instance with the Email Filters plugin.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) Email filters enable administrators to use a condition builder or conditional script to specify when to ignore malicious incoming emails from known/unknown sender.</td>
</tr>
</tbody>
</table>
| References                       | Email filters

https://support.servicenow.com/kb_view.do?sysparm_article=KB0549426

To learn more about activating a plugin, see Activate a plugin.

Restrict access to emails with empty target table (instance security hardening)

Activate the `glide.email.email_with_no_target_visible_to_all` property to restrict user access to emails, unless they were the one who sent the email, or have an admin role.

Unauthorized users are able to access emails in the `sys_email_list` table that are missing a target record. Instead of enforcing ACLs on email entries, this property restricts access only to the email sender, and users with the admin role.
Note: Emails sent to and received by the instance and received appear in the sys_email_list table. However, only received emails that were marked with an Error and Ignored state should have an empty target table.

More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.email.email_with_no_target_visible_to_all</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To block email client from showing emails when user doesn't authorize access.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>false</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) Users are no longer able to see emails where target table is empty unless they are an admin or were the sender of the email.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) If the property is not enabled, unauthorized users are able to access any email where the target_table field is empty.</td>
</tr>
<tr>
<td>References</td>
<td>Advanced email properties <a href="https://support.servicenow.com/kb_view.do?sysparm_article=KB0690043">https://support.servicenow.com/kb_view.do?sysparm_article=KB0690043</a></td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.

Restrict emails by domain for user creation (instance security hardening)

Use the glide.user.trusted_domain property to specify the comma-separated list of trusted domains used in the creation of users from incoming emails.

By default, an asterisk (*) is used to trust all domains. Specific domains should be provided if it is not required to allow email from every domains. The instance ignores incoming email from other domains unless it is from an existing user's address. The instance doesn't create guest users from email from untrusted domains.

Prerequisites

Before setting this property:

- Set the glide.email.read.active property to true. To learn more, see Enable using your own POP3 server.
- Set the glide.pop3readerjob.create_caller property to true. To learn more, see Enable automatic user creation.

Note: Skip the glide.user.default_password property if the glide.pop3readerjob.create_caller property is set to false.
More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.user.trusted_domain</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To restrict the inbound emails coming from domains that included are not in the trusted domain list.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>Comma-separated list of trusted domains [Ex. servicenow.com (a specific domain name)]</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Medium) Once this property is configured, the instance no longer accepts emails from untrusted domains. If you do not include the domain in the trusted list, there is an impact to guest users because accounts are created automatically.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) If the property is not enabled, an attacker might use an email spoofing/spamming campaign to send multiple emails resulting in the creation of more unnecessary guest users.</td>
</tr>
<tr>
<td>References</td>
<td>Email properties</td>
</tr>
<tr>
<td></td>
<td>Inbound mail configuration</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.

Set complex default password (instance security hardening)

Use the glide.user.default_password property to specify the password for new users created from incoming email from trusted domains.

Although this password resets during login, a complex custom password must be applied instead of the default value 'password'. The instance ignores incoming email from other domains unless it is from an existing user's address. The instance doesn't create guest users from email from untrusted domains.

Prerequisites

Before setting this property:

- Set the glide.email.read.active property to true. To learn more, see Enable using your own POP3 server.
- Set the glide.pop3readerjob.create_caller property to true. To learn more, see Enable automatic user creation.

Note: Skip the glide.user.default_password property if the glide.pop3readerjob.create_caller property is set to false.
More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.user.default_password</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To enforce strict unique temporary password for the user created on domains specified in the inclusion list.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>Unique Password [Ex. MyComp@ny123! (with strong password complexity)]</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) No impact on users. Instead of default password user created has to log in with initial unique password set by admin.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) Service sets the default password across all the zbooted/newly provisioned instance. Change the default credentials because an attacker might guess the legitimate user created from an inbound email with default temporary password to gain access to that user account.</td>
</tr>
<tr>
<td>References</td>
<td>Available system properties, Email properties, Inbound mail configuration</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.

Input validation (instance security hardening)

The Now Platform performs input validation to prevent issues that result from the entry of malformed data. This section describes security controls within the Now Platform that an administrator can configure to minimize entry of malformed data, regardless of source. These sources include manual user entry, or from an infrastructure, external entities, or database systems.

Allow embedded HTML code (instance security hardening)

Use the glide.ui.security.allow_codetag property to disable support for embedding HTML code created using the [code] tag.

The Now Platform mitigates many injection and cross-site attacks by implementing escaping and encoding techniques. As a result, users can't write/submit HTML formatted inputs for journal fields. But journal fields can render text enclosed within code tags as HTML.

- However, there is an associated security risk. If set to true, malicious users can write harmful HTML JS code that may be executed on a different client browser after rendering of journal fields.
- Set this property to false so that administrators can prevent journal fields from rendering HTML code by disabling support for the [code] tag.
More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.ui.security.allow_codetag</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>Protect against cross-site scripting and malicious script execution</td>
</tr>
<tr>
<td>Recommended value</td>
<td>false</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Medium) This remediation enforces HTML encoding to occur on the UI and renders the encoded results to the user. This property is set to true by default. In this state, your instance displays rendered HTML in journal fields and forms. If this property is set to false, HTML is not rendered properly and HTML tags may appear in journal fields on forms. It can have an adverse impact on functionality, and on user interactions with the resulting data.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) Input validation must occur in the application to defend against cross-site scripting attacks. These attacks enable foreign scripts to execute on user session in the logged in browser's context. Attackers can use it to steal session information and sensitive data.</td>
</tr>
<tr>
<td>References</td>
<td>Restrict the CODE tag in journal fields</td>
</tr>
<tr>
<td></td>
<td>Render journal field entries as HTML</td>
</tr>
<tr>
<td></td>
<td>High Security Settings</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see [Add a system property](#).

**Allow JavaScript tags in embedded HTML (instance security hardening)**

Use the glide.ui.security.codetag.allow_script property to disable support for embedding HTML JavaScript code created using of the [code] tag.

The Now Platform mitigates many injection and cross-site attacks by implementing escaping and encoding techniques. As a result, users can't write and submit HTML formatted inputs for journal fields. However, journal fields can render text enclosed within code tags as HTML.

- However, there is an associated security risk. If set to true, malicious users can write harmful HTML JavaScript code that may be executed on a different client browser after rendering of journal fields.
- Set this property to false so that administrators can prevent journal fields from rendering HTML JavaScript code by disabling support for the [code] tag.

More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.ui.security.codetag.allow_script</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>Protects against cross-site scripting and malicious script execution</td>
</tr>
<tr>
<td>Recommended value</td>
<td>false</td>
</tr>
<tr>
<td>Functional impact (Medium)</td>
<td>This remediation enforces JavaScript escaping to occur on the UI and renders the encoded results to the user. It can have a functionality impact based on the instance user interaction with the resulted data.</td>
</tr>
<tr>
<td>Security risk (High)</td>
<td>Input validation must occur in the application to defend against cross-site scripting attacks. These attacks enable foreign scripts to execute on the user session in the logged in browser's context. Attackers can use it to steal session information and sensitive data.</td>
</tr>
<tr>
<td>References</td>
<td>Restrict the CODE tag in journal fields</td>
</tr>
<tr>
<td></td>
<td>Render journal field entries as HTML</td>
</tr>
<tr>
<td></td>
<td>High Security Settings</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.

**Client generated scripts sandbox (instance security hardening)**

Use the `glide.script.use.sandbox` property to enable script sandboxing.

There are two cases in the Now Platform that enable the client to send scripts to the server for evaluation:

**Filters or queries**

It is legal to send a filter to the server such as `assigned_to=JavaScript:getMyGroups()`.

**System API**

API call enables the client to run arbitrary scripts on the server and receive a response.

If you enable script sandboxing, the script being evaluated at either of these two entry points runs in a sandbox with reduced rights, with the following characteristics:

- Only those business rules marked client callable are available within the sandbox.
- Only script includes marked client callable are available within the sandbox.
- Certain API calls (largely, but not entirely, limited to ones dealing with direct DB access are not allowed.
- You can't insert, update, or delete data from within the sandbox. For example, any calls to `current.update()`, are ignored. If you run the Now Platform without enabling script sandboxing, none of these restrictions apply.

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.script.use.sandbox</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Purpose</td>
<td>Enforces validation for the client-side JavaScript queries that are launched against the platform</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(High) This remediation enforces validation for the client-side JavaScript queries that are launched against the Now Platform. There is a potential impact if customer has customizations that include hard-coded JavaScript queries to perform CRUD operations.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(High) The Now Platform provides wide variety of features and functionality through JavaScript queries. However, without appropriate authorization and validation, there is a potential for an attacker to perform unauthorized operations against the platform.</td>
</tr>
</tbody>
</table>
| References           | Script sandbox property

**glide.script.use.sandbox** belongs to the same family of properties that secure and restrict execution of scripts originating from the client:

- **glide.script.allow.ajaxevaluate**: See Enable AJAXEvaluate.
- **glide.script.secure.ajaxgidererecord**: See Enabling AJAXGlideRecord ACL checking (instance security hardening).

To learn more about adding or creating a system property, see Add a system property.

**Enable AJAXEvaluate (instance security hardening)**

Use the **glide.script.allow.ajaxevaluate** property to restrict arbitrary client script execution using the system API on the server side.

There are two cases in the Now Platform that enable the client to send scripts to the server for evaluation:

- **Filters and/or queries**
  It is legal to send a filter to the server such as: `assigned_to=javascript:getMyGroups()`

- **System API**
  The AJAXEvaluate API call allows the client to run arbitrary scripts on the server and receive a response.

When you set this property to **false**, the Now Platform doesn't enable the use of the AJAXEvaluate API call from the client script.

**More information**
### Attribute | Description
--- | ---
**Functional impact** | (Medium) This remediation forces the AJAEvaluate processor to be turned off. It could impact functionality if you are explicitly using the AJAX evaluate processor as part of any customized scripts. For more information, see GlideAjax.

**Security risk** | (High) AJAXEvaluate can allow arbitrary JavaScript code to execute on the client browser by applying the server-side objects.

### References
- **Script sandbox property**
  - **GlideAjax**
  - **glide.script.allow.ajaxevaluate** belongs to the same family of properties that secure and restrict execution of scripts originating from the client:
    - **glide.script.use.sandbox**: See Client generated scripts sandbox.
    - **glide.script.secure.ajaxgliderecord**: See Enabling AJAXGlideRecord ACL checking.

To learn more about adding or creating a system property, see [Add a system property](#).

### Escape Excel formula (instance security hardening)
Use the **glide.export.escape_formulas** property to prevent Excel Injection, also, known as formula injection.

Excel injection occurs when websites embed untrusted entries inside Excel files. When you use a spreadsheet application such as Microsoft Excel, or LibreOffice Calc, to open a file, any cells starting with +, -, =, or @ are interpreted as a formula. When you set the **glide.export.escape_formulas** property to **true**, string values starting with +, -, =, or @ are prepended with a single apostrophe when you export to CSV, XLS, or XLSX files.

### More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td><strong>glide.export.escape_formulas</strong></td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To prevent application against the Excel or formula injection.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) Maliciously crafted formulas can be used for hijacking the user's computer by exploiting vulnerabilities in the spreadsheet software.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) Malicious formulae pose a risk even when the embedding spreadsheet doesn't contain any sensitive information, as they can be used to compromise the viewer's computer.</td>
</tr>
<tr>
<td>Workaround</td>
<td>As an alternative consider stripping all trailing white spaces where possible, and limiting all client-supplied data to alpha-numeric characters.</td>
</tr>
</tbody>
</table>
To learn more about adding or creating a system property, see Add a system property.

Escape HTML (instance security hardening)

Use the glide.ui.escape_html_list_field property to force HTML escapes for HTML fields in a list view.

HTML is one of the types that can be assigned to the dictionary fields. Assigning HTML fields to any field type provides the functionality to format content using HTML codes (for example, `<p>`, `<a href>`, `<b>`, `<font>`, `<img>`). A malicious user can inject HTML code within the form field to execute unwanted scripts on different client/user sessions.

- Set this property to true to perform an HTML escaping before the records/fields are rendered in the browser when the table appears as a list view.
- If set to false, and you select that column in a list view when viewing a table or record listing, these HTML formatted fields may appear.

More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.ui.escape_html_list_field</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To prevent application against cross-site scripting attacks</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Medium) This remediation enforces HTML encoding to occur on the UI at the HTML parser level and thus renders back encoded results to the user. It can have a functionality impact based on the instance user interaction with the resulted data.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(High) Input validation must occur on the application to defend against cross-site scripting attacks. These attacks enable foreign scripts to execute on user sessions in the logged in browser's context. Attackers can use it to steal session information and sensitive data.</td>
</tr>
</tbody>
</table>

References: High Security Settings

To learn more about adding or creating a system property, see Add a system property.

Escape JavaScript (instance security hardening)

Use the glide.html.escape_script property to force escape from JavaScript (`<script>`</script>) tags in HTML fields during list views.

HTML is one of the types that can be assigned to the dictionary fields. Assigning HTML fields to any field type provides functionality to the user to format the content using HTML codes (for example, `<p>`, `<a href>`, `<b>`, `<font>`, `<img>`). If you set glide.html.escape_script to false, the (`<script>`</script>) tags may appear when you select that column in a list view while viewing a table or record listing.
A malicious attacker can insert JavaScript code by embedding it within the `<script></script>` tags. The attacker can take advantage by injecting a sophisticated JS vector that may execute when any user opens the table record.

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.html.escape_script</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To prevent cross-site scripting attacks against an application.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Medium) This remediation enforces JavaScript escaping to occur on the UI and renders encoded results to the user. It can have an impact on functionality, based on the instance user interaction with the resulting data</td>
</tr>
<tr>
<td>Security risk</td>
<td>(High) Input validation must occur in the application to defend against cross-site scripting attacks. These attacks enable foreign scripts to execute on user session in the logged in browser's context. Attackers can use it to steal session information and sensitive data.</td>
</tr>
<tr>
<td>References</td>
<td>Available system properties</td>
</tr>
<tr>
<td></td>
<td>High Security Settings</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.

**Escape Jelly (instance security hardening)**

Use the `glide.ui.escape_all_script` property to force escape of all scripts injected into Jelly.

It escapes all the JS and HTML strings included in `<j:jelly> ... </j:jelly>` before they are written to the output stream, preventing several XSS issues from occurring.

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.ui.escape_all_script</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Attribute Description

**Purpose**
If the property is not set to `true`, developers have to perform several steps on each custom Jelly script to prevent XSS issues. These steps include locating the Jelly variables being sent to output stream to render on web pages, and performing escaping on each of the following tags:

- `$$ {JS:expression}`
- `$$ {HTML:expression}`

OR
- `$$ {JS,HTML:expression}`

**Recommended value**
true

**Functional impact**
(Medium) This remediation enforces Jelly escaping at the parser level. It can have a functionality impact on user interaction with the resulting data.

**Security risk**
(High) Input validation has to occur on all the user input being entered on the application. By doing so, injection attacks against the platform can be defended and protected.

**Workaround**
The UI may be affected because some of the scripts and HTML tags designed for rendering on a web page may appear broken. This remediation sends the output encoded page to the browser to render. For example, instead of 'my string here', it might display `<u>my string here</u>` as the `<u>` tag was properly escaped. In this case, to prevent escaping, add the NOESC prefix to Jelly expression to prevent JS escaping. For example:

- Before: `($[jvar_context_menus]);`
- After: `($[NOESC:jvar_context_menus]);`
- Before: `[$[jvar_ui_policy_scripts]`
- After: `($[NOESC:jvar_ui_policy_scripts]`

**References**
- High Security Settings
- Jelly tags

To learn more about adding or creating a system property, see [Add a system property](#).

### Escape XML (instance security hardening)

Use the `glide.ui.escape_text` property to force escape of XML values at the parser level before transmitting them to the client's browser.

Cross-site scripting occurs when an attacker injects malicious JavaScript into an entry point. The platform/application fails to escape the malicious JavaScript before transmitting it to the victim's browser for execution. Escaping in this context means the following:

- `&` --> `&amp;`
- `<` --> `&lt;`
- `>` --> `&gt;`
- `"` --> `&quot;`
- `'` --> `&#x27;`
Example: `<script>alert('XSS Attack');</script>`

Escaping: `<script>alert('XSS Attack');</script>`

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.ui.escape_text</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>Escaping XML ensures that browsers do not parse the malicious JavaScript embedded in untrusted data, and execute it as JavaScript.</td>
</tr>
<tr>
<td></td>
<td>• A malicious user may try XSS attack to either hijack other users' session or redirect the user to a malicious website.</td>
</tr>
<tr>
<td></td>
<td>• The Now Platform contains code to secure cookies, but escaping it relies on this property being set to <code>true</code>.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Medium) This remediation enforces XML encoding at the XML parser level on the UI. It renders the encoded results for the user, which can have a functionality impact based on the instance user interaction with the resulted data.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(High) Input validation must occur on the application to defend against cross-site scripting attacks. These attacks enable foreign scripts to execute on user session in the logged in browser's context. Attackers can use it to steal session information and sensitive data.</td>
</tr>
<tr>
<td>Workaround</td>
<td>After you set this property to <code>true</code>, rendering stops on the HTML tags in the catalog item description or in the catalog item variable help text. You may not be able to use HTML formatting for some fields. However, if the <code>glide.ui.escape_text</code> property is turned off, all JEXL expressions would be prefixed with an output encoder:</td>
</tr>
</tbody>
</table>
|                                        |    ```jsp
|                                        |    ${JS:expression}
|                                        |    ${HTML:expression}
|                                        |    or
|                                        |    ${JS,HTML:expression}
| References                             | High Security Settings                                                                                                                       |

To learn more about adding or creating a system property, see Add a system property.
HTML sanitizer (instance security hardening)

Use the `glide.html.sanitize_all_fields` property to enable the HTMLSanitizer script include, which sanitizes HTML input based on exclusion listed and inclusion listed attributes configured in a script.

The field types available with dictionary/fields include HTML and Translated HTML. These HTML input fields enable users to write HTML formatted input, for example:

```html
<h1>Test</h1>, using the most basic HTML tags such as `<img>`, `<a href ...>`, and `<iframe>`.
```

It can open a door for a malicious attacker to inject malicious vector with HTML tags such as:

```html
[<IMG SRC=" &amp;#14; JavaScript:alert('XSS');">][<IMG onmouseover="alert('xss')">][a href="" onclick=alert(/xss/)].
```

### More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.html.sanitize_all_fields</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security</td>
<td>Yes</td>
</tr>
<tr>
<td>Center</td>
<td></td>
</tr>
<tr>
<td>Purpose</td>
<td>Prevents application against cross site scripting and HTML injection attacks</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(High) This remediation enforces HTML-output encoding mechanism before the user data is rendered back to the user. If customer has any customization that involves rendering of the HTML attribute or content data, then there is a functionality impact.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(High) User input should be securely treated when the data is being stored and processed on the application. This reduces client-side cross-site scripting attacks by output encoding the data.</td>
</tr>
<tr>
<td>Workaround</td>
<td>This property sanitizes all HTML fields in the system. If you must enable HTML sanitization on individual fields, see Enable sanitization on individual fields. You can also configure the inclusion list or exclusion list to sanitize HTML tags and attributes as per your organizations policy.</td>
</tr>
<tr>
<td>References</td>
<td>Enable HTML sanitizer</td>
</tr>
<tr>
<td></td>
<td>HTML sanitizer</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.

Jelly/JS interpolation (instance security hardening)

Use the `glide.ui.jelly.js_interpolation.protect` property to ensure that any JavaScript about to be executed on a Jelly page is protected from injection with the help of Jelly interpolation.

When you set property to `true`, an application goes through a Jelly script tree (nested). It wraps potentially dangerous Jelly expressions with a filter that:

- Escapes their results to be safe, or
• If their safety can't be guaranteed, generates a SecurityException because the expression that was going to be evaluated represents a possible security issue.

More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.ui.jelly.js_interpolation.protect</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To mitigate against malicious code execution attacks that can occur using Jelly Injection.</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(High) This property makes a best guess at whether an expression is quoted. It may wrongly quote legitimate expression. In that case manually marking an expression as safe may be necessary.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) JEXL injection is a form of input injection unique to the Now Platform that can lead to both cross-site request forgery and code execution. Completely turning off the protection may potentially open many P1 security vulnerabilities.</td>
</tr>
<tr>
<td>Workaround</td>
<td>To manually mark an expression as safe add SAFE prefix to Jelly expression: $(SAFE:sysparm_input); Blindly adding SAFE to each expression is the wrong way to approach the problem, because it may open a security vulnerability.</td>
</tr>
<tr>
<td></td>
<td>• Only add SAFE to an expression if you can guarantee that the expression does not contain input from the client.</td>
</tr>
<tr>
<td></td>
<td>• If it does, it's possible for a malicious client to cause evaluation of privileged JavaScript.</td>
</tr>
</tbody>
</table>

References

- Jelly tags
- High Security Settings

To learn more about adding or creating a system property, see [Add a system property](#).

**SOAP request strict security (Instance security hardening)**

Use the `glide.soap.strict_security` property to enforces web service security. This property uses a combination of:

• Basic authentication challenge/response over the HTTP protocol and
• System level access controls in the [Contextual Security: Role Management plugin](#).

If you set this property to `true`, it performs the following actions:

• If the user has appropriate role to perform the operation, it checks incoming SOAP request for role authorization to validate. It occurs during SOAP web service calls/requests made against Now Platform tables when performing CREATE, READ, UPDATE or DELETE operations.
• Checks the system-level ACLs while retrieving data in the form of SOAP data on the table.
• Checks the field-level ACLs for any CRUD operation performed against a field of table

More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.soap.strict_security</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>Ensure security ACLs are checked and validated even when the records are accessed through SOAP calls</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(High) This remediation enforces the system-level access control while retrieving data from tables/pages in the form of SOAP data on the instance. If there are users currently accessing this data, they are restricted/allowed to access the data based on the ACL rules. For the default roles that have access to the SOAP data, see SOAP Roles.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(High) Without appropriate authorization configured on the incoming SOAP requests, an unauthorized user can get access to sensitive content/data on the target instance.</td>
</tr>
<tr>
<td>References</td>
<td>Enforce strict security for inbound SOAP SOAP web service</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.

Secure communications (instance security hardening)

The secure communication properties relate to the security of the transportation of HTTP traffic.

Certificate trust (instance security hardening)

By default, the com.glide.communications.trustmanager_trust_all property is set to false. The Now Platform only trusts certificates that it can verify against the JVM certificate store. Self-signed and enterprise-signed certificates are not trusted.

Note: For security purposes, do not change this property value. If you have further questions, contact Customer Service and Support.

More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>com.glide.communications.trustmanager_trust_all</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To enforce certificate validation for outgoing requests.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>false</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Medium) This remediation enforces strict validation on certificate CA field. If a trusted entity(CA) issued the certificate, the instance accepts it for further use.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) For confidentiality and integrity reasons, application should validate the certificate's CA before using the certificate for any transactional operations.</td>
</tr>
<tr>
<td>References</td>
<td>Certificates</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.

**Disabling SSLv2/SSLv3 (instance security hardening)**

Use the `glide.outbound.ssvl3.disabled` property to force the MID Server to use TLS when making outbound connections, such as REST and SOAP requests. Normally, outbound connections from an instance are forced to use TLS instead of SSL.

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td><code>glide.outbound.ssvl3.disabled</code></td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To enforce the use if TLS during all outbound connections from ServiceNow instance.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Medium) This remediation enforces the usage of TLS protocol version when communicating on HTTPS. If there are devices that customer/users of the instance are using that do not support TLS communication, there may be a potential outage.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) Legacy versions of SSL were proven to be insecure when utilized for HTTP secure shell implementation, due to client-side attacks, including BEAST and SSL heart-bleed.</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.
Security best practices (instance security hardening)

In addition to security configurations, some extra manual effort is required to further secure Now Platform applications on a day-to-day basis. This section contains security tasks that an administrator should perform periodically, within a certain interval of time.

Cache-Control HTTP header value (instance security hardening)

Use the `glide.http.cache_control` property to set the default Cache-Control value in the HTTP response headers that the Now Platform sends when requesting static content data for a page. Examples of static content include images, CSS, and JavaScript rendered from within, for a page.

The `glide.http.cache_control` property sets the default Cache-Control value in HTTP response headers to **private** or **public**. The default is **private**.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>private</td>
<td>Static content can be cached at the browser (client) level, but not at the proxy server level.</td>
</tr>
<tr>
<td>public</td>
<td>Static content can be cached at the browser (client) level, and also at the proxy server level.</td>
</tr>
</tbody>
</table>

The Expires value in the HTTP response headers control when the static content expires, and has a default value of 369 days. To manually override the default value, use the `glide.http.expire.days` property.
Note: You can use the `glide.http.cache` property to designate whether to enable or disable setting of the Cache-Control and Expires values in HTTP response headers. Its default is `true`, which allows you to set the:
Cache-Control value default using the glide.http.cache_control property.
Expires value default using the glide.http.expire.days property.

More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.http.cache_control</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To configure the Cache-Control HTTP response header value for static content.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>private</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Medium) Sets the default Cache-Control value in an HTTP response header.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(High) If you set this property to public, instances with CDN/proxies may cache static content and render without authentication.</td>
</tr>
<tr>
<td></td>
<td>• private is a more appropriate setting for instances with CDN/proxy setup.</td>
</tr>
<tr>
<td></td>
<td>• If an the instance does not have a CDN(proxy setup, either value should be fine.</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.

High security plugin (instance security hardening)

When you activate the High Security plugin, it creates or updates hundreds of different configurations to control the level of security on your instance. These configurations mitigate many of the top OWASP attacks by enabling strict access control, input validation, and output encoding.

These configurations include:
• Access Control
• Business rules
• System properties
• UI policy action
• script actions
• script includes

Example

Refer to the examples for the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.ui.escape_all_script</td>
<td>Escape Jelly</td>
</tr>
</tbody>
</table>
## More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plugin Name</td>
<td>com.glide.high_security</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Definition &gt; Plugins - Development</td>
</tr>
<tr>
<td>Purpose</td>
<td>It is mandatory to activate this plugin. It increases the security level of</td>
</tr>
<tr>
<td></td>
<td>an instance, which reduces the attack surface by mitigating owasp top 10</td>
</tr>
<tr>
<td></td>
<td>attacks, including CSRF, XSS, Securing Session Cookies, and File uploads.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>Active</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(High) This plugin enables several system security configurations,</td>
</tr>
<tr>
<td></td>
<td>which may impact UI and functionality as well.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(High) Many security configurations are unintentionally left open,</td>
</tr>
<tr>
<td></td>
<td>which may open the door for some of the critical vulnerabilities.</td>
</tr>
<tr>
<td>References</td>
<td>Request High Security Settings activation</td>
</tr>
<tr>
<td></td>
<td>High Security Settings</td>
</tr>
</tbody>
</table>

To learn more about activating a plugin, see [Activate a plugin](#).

### Individual login IDs (instance security hardening)

Ensure that all users have individual user IDs, which enables auditing of all user activities.

**Note:** Local user accounts that are not being used should have the **Active** flag set to false.

- Setting the **Active** flag to **false** automatically sets the **Locked Out** flag to **true**. If the **Locked Out** flag is set to **true**, it doesn't allow that user account to authenticate to the instance.
- Setting the **Active** flag to **false** does not remove a user from the Now Platform, but does remove visibility to non-admin accounts.
- If **Active** flag is set to **false**, and **Locked Out** flag is also set to **false**, a user still is able to log in to this account.

To learn more about user accounts, see [User administration](#).
Mobile UI obfuscation (instance security hardening)

Use the `glide.ui.m.blur_ui_when_backgrounded` property to obfuscate all fields from the snapshot as the image is saved during the backgrounding process. To obfuscate.

On Android devices, the Android operating system takes a screenshot for usage in the recent task menu when the application is sent to background. Users can also take manual screenshots of the application, which are stored publicly on the device.

On iOS devices, the iOS operating system also allows applications to save an image file. This file represents the last screen seen by the user when the application is sent to the background. While the intent is to provide a better user experience, it also creates a security risk because the images are saved as PNG image files.

**Note:** This setting or configuration is per instance basis so the user must connect to the instance with the property configured.

To obfuscate all fields from the snapshot in the ServiceNow Classic app, see Configure the blur app option to improve security.

**Example**

When you set this property to **true**, Background application is obfuscated for iOS devices, and blacked out for Android iOS devices.
More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property/Plugin Name</td>
<td>glide.ui.m.blur_ui_when_backgrounded</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Nos</td>
</tr>
<tr>
<td>Purpose</td>
<td>To obfuscate all fields from the snapshot as the image is saved during the backgrounding process.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
</tbody>
</table>
### Attribute

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional impact</td>
<td>(Low) If the <code>glide.ui.m.blur_ui_when_backgrounded</code> property is set to <code>true</code>, the native apps use the parameter defined on the server to blur the screen when the app enters the background.</td>
</tr>
<tr>
<td></td>
<td>• It blurs the screenshots taken by iOS and Android when the app enters the background.</td>
</tr>
<tr>
<td></td>
<td>• The user experience may be adversely affected because they would not be able to see the content when the app is sent to background.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) A compromised (jailbroken) device would enable an attacker to have full access to the file system, with access those files/snapshots with sensitive information embedded in them.</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see [Add a system property](https://support.servicenow.com/kb_view.do?sysparm_article=KB0550107).

### Patches and updates (instance security hardening)

Ensure that the instance is running the most current patch level. Security fixes are routinely released for the Now Platform within many of the patches and hot fixes that accompany product feature updates. Upgrading when new patches and hot fixes are available reduces the risk of potential vulnerabilities.

The Now Platform undergoes two penetration tests per week on average.

- While most of these tests do not result in significant vulnerabilities, there are vulnerabilities found and fixed regularly.
- Information about Now Platform releases, patches, and hot fixes can be found in the Release Notes section of the product documentation.

### Remove demo data (instance security hardening)

Demo data, particularly demo accounts, are typically included when an instance is created. If so, all demo data should be removed prior to using the instance in non-production or production.

Open a request in HI. Make sure to create an administrative account prior to submitting the request.

### Internal resources

- [https://support.servicenow.com/kb_view.do?sysparm_article=KB0550107](https://support.servicenow.com/kb_view.do?sysparm_article=KB0550107)

### Removing demo data using the Service Catalog

Instead of submitting the request as an incident, certain users can request demo data removal on an instance using the Service Catalog. These users include internal users, and those users who have customer admin or partner admin roles,

1. Navigate to [https://support.servicenow.com/hisp](https://support.servicenow.com/hisp).
2. Click **Self-Service > Remove Demo Data >**.
3. Specify the instance from which to remove demo data.
   - If you are having trouble finding your instance, preface the instance name with * to perform a contains query.
4. Specify the date and time to remove demo data from the selected instance.
The date and time must be at least four hours later than the current time.

5. Click **Submit**.

A new change request is created and appears automatically. The **Planned end date** is automatically calculated based on the **Planned start date** plus five hours, which is how long the process takes. In the change request, use the Watch List to add any other members of your team who must be aware of the change request status.

### Security inclusion listing (instance security hardening)

A 'positive' security model (also known as an 'inclusion list') is one that defines what is allowed, and rejects everything else. This section contains security controls that an administrator can configure to restrict behavior to known inclusion lists.

### Check allow list member calls (instance security hardening)

Review and remove inclusion list member call entries as needed from the sys_whitelist_member table.

Member call entries can access the Java resources on the server-side to perform application-based operations without appropriate validation. Because it can cause unauthorized disclosures or alteration of customer data, it is a serious security concern.

### More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table Name</td>
<td>sys_whitelist_member</td>
</tr>
<tr>
<td><strong>Note:</strong> In recent releases, only ServiceNow employees can access this table; not even administrators are able to do so.</td>
<td></td>
</tr>
<tr>
<td>Configuration type</td>
<td>Table</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To review and remove entries from this table.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>No record should exist in the table (the list must be empty).</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) There should be no impact as long as you review and approve the results generated when running the Packages call removal tool. To ensure proper functioning of the instance, test the changes in a non-production environment before deploying in the production environment. To learn more, see Packages call removal tool.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(High) client-side API calls that result in data retrieval or object access on server are deemed to be dangerous from a security standpoint. Validate these items for authorization and restriction of sensitive object access.</td>
</tr>
</tbody>
</table>

### Steps to configure

**Note:** The following steps are similar to the steps outlined in the Steps to Configure sections in:
• Packages call removal tool
• Check whitelist package calls

If you already completed them, you can skip these steps.

1. Activate the Packages Call Removal Tool plugin. To learn more, see Packages call removal tool.
2. Using filter navigator, navigate to **Packages Call Removal Utility**.
3. Click each script starting from (1) to (4). Wait for the output, then proceed to the next one.
4. Once you run the script (4), a listing of affected fields appears on the Packages Call Items page.

5. Resolve all the items in the Proposed and Error sections.

**Note:** This tool might report some package calls used in `sa_mapping_ext_commands` and `sa_custom_operation`. These package calls belong to the MID Server. Because there are no classes, the code runs in MID Server. If you find the following member calls under the Errors section, mark them as **Rejected** (Ignored). The tool doesn't report that member call again.

- Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_content);
- Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_name);
- Packages.com.snc.sw.commands.HttpCallHandler;
- Packages.com.snc.sw.dto.ProviderType.SSH

6. Contact ServiceNow Support for further remediation.

**Check allow list package calls (instance security hardening)**

Review and remove inclusion list package call entries as needed from the `sys_whitelist_package` table.

Package call entries can access Java resources on the server-side to perform application-based operations without appropriate validation. Because it can cause unauthorized disclosures or alteration of customer data, it is a serious security concern.

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table Name</td>
<td><code>sys_whitelist_package</code></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> In recent releases, only users with a maint role can access this table; not even administrators are able to do so.</td>
</tr>
<tr>
<td>Configuration type</td>
<td>Table</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To review and remove entries from this table.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>No record should exist in the table (the list must be empty).</td>
</tr>
<tr>
<td>Functional impact</td>
<td><em>(Low)</em> There should be no impact as long as the results from running the Packages call removal tool are reviewed and approved. To ensure proper functioning of the instance, test the changes in a non-production environment before deploying in the production environment. To learn more, see Packages call removal tool (instance security hardening).*</td>
</tr>
<tr>
<td>Security risk</td>
<td><em>(High)</em> client-side API calls that result in data retrieval or object access on server are deemed to be dangerous from a security standpoint. Validate these items for authorization and restriction of sensitive object access.</td>
</tr>
<tr>
<td>Workaround</td>
<td>Contact ServiceNow Support for assistance.</td>
</tr>
</tbody>
</table>
Steps to configure

1. Activate the Packages Call Removal Tool plugin. To learn more, see Packages call removal tool.
2. Using filter navigator, navigate to Packages Call Removal Utility.
3. Click each script starting from (1) to (4). Wait for the output, then proceed to the next one.
4. Once you run the script (4), a listing of affected fields appears on the Packages Call Items page.

5. Resolve all the items in the Proposed and Error sections.

   **Note:** This tool might report some package calls used in `sa_mapping_ext_commands` and `sa_custom_operation`. These package calls belong to the MID Server. Because there are no classes, the code runs in MID Server. If you find the following package calls under the Errors section, mark them as **Rejected** (Ignored). The tool doesn’t report that package call again.

   - `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_content);`
   - `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_name);`
   - `Packages.com.snc.sw.commands.HttpCallHandler;`
   - `Packages.com.snc.sw.dto.ProviderType.SSH`

6. Contact ServiceNow Support for further remediation.

---

**Enable URL allow list for cross-origin iframe communication (instance security hardening)**

Use the `glide.ui.concourse.onmessage_enforce_same_origin` property to enable cross-origin communication between iframes.

Openframe can only process messages from trusted domains that are specified in the `glide.ui.concourse.onmessage_enforce_same_origin_whitelist` property. To learn more, see Specify URL whitelist for cross-origin iframe communication.

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td><code>glide.ui.concourse.onmessage_enforce_same_origin</code></td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To enable inclusion listing of trusted domains, so they can communicate between iframes for openframe.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Medium) If you do not inclusion list intended domains, the ability to embed other pages within Now Platform instances may be limited.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(High) If a web page contains event handlers that do not perform proper origin validation, a web page, or script from any origin, can communicate with it. It can also initiate any functionality performed by the event handler.</td>
</tr>
<tr>
<td>References</td>
<td><a href="#">OpenFrame overview</a></td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see [Add a system property](#).

**Enforce relative links (instance security hardening)**

Use the `glide.cms.catalog_uri_relative` property to enforce relative links from the URI parameter on `/ess/catalog.do`. 
• If you set the property to **true**, only relative URLs are permitted through the `/ess/catalog.do` page using the `uri` parameter.

If you set it to **false**, all URLs are permitted, which may permit linking to external unauthorized content.

### More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.cms.catalog_uri_relative</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To restrict attempts to link external unauthorized content.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td><em>(Low)</em> This remediation enforces validation on Catalog page such that only Relative URLs are permitted. Existing links to external web applications become broken.</td>
</tr>
<tr>
<td>Security risk</td>
<td><em>(Medium)</em> Absolute URLs can pose a security risk when used as a part of parameter or a field value, thus redirecting the source page to an adversary-controlled website.</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see [Add a system property](#).

### Packages call removal tool (instance security hardening)

Activate and run the Packages Call Removal Tool (`com.glide.script.packages_call_removal`) plugin, and then consider whether each of the proposed changes should be completed or rejected.

The Packages Call Removal Tool is a plugin that:

- Scans scripts for package calls to Now Platform Java classes.
- Proposes changes to replace them with preferred GlideScriptable names.
- Facilitates the script changes.

**Note:** If this record is a base system record, using the recommendation from the tool causes the item to be marked as customer_update. That script may not take on further updates in the future. In later releases, the `sys_whitelist.xxx` tables are expected to be empty. However, it may still be useful to use this tool because it flags `Packages.xxx` calls.

The Packages Call Removal Tool might report some package calls used in `sa_mapping_ext_commands` and `sa_custom_operation`. These package calls belong to the MID Server. As there are no classes, the code runs in MID Server. If you find any of the following listed package calls in the Errors section, mark them as Rejected (Ignored). The tool doesn't report that package call again.

- `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_content);`
- `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_name);`
- `Packages.com.snc.sw.commands.HttpCallHandler;`
- `Packages.com.snc.sw.dto.ProviderType.SSH`
More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plugin Name</td>
<td>com.glide.script.packages_call_removal</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Definition &gt; Plugins</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To remove/replace unauthorized package/member calls with Glide Acceptable (GlideScriptable) names that only allow authorized access to data.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>Active</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) This remediation would replace the package calls with GlideScriptable APIs, and can affect the customizations that include package calls. The tool doesn’t actually replace package calls automatically. Instead, it provides suggestions that are stored into the packages_call_item table. Your administrator can then decide whether to accept or reject the proposed change.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) Client-side API calls that result in data retrieval or object access on server are deemed to be dangerous from a security standpoint. They should be validated for authorization and restriction for sensitive object access.</td>
</tr>
</tbody>
</table>

Steps to configure

1. Navigate to System Definition > Plugins
2. Search for the plugin ID = `com.glide.script.packages_call_removal`. 
3. Click **Activate/Upgrade** to activate the plugin.
4. To check inclusion list package calls and inclusion list member calls, complete the actions outlined in the Steps to Configure sections in the following topics:
   - Check whitelist member calls
   - Check whitelist package calls

**Specify URL allow list for cross-origin iframe communication (instance security hardening)**

Use the `glide.ui.concourse.onmessage_enforce_same_origin_whitelist` property to enable cross-origin communication between iframes from trusted domains you specify in an inclusion list.

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.ui.concourse.onmessage_enforce_same_origin_whitelist</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>No</td>
</tr>
<tr>
<td>Purpose</td>
<td>To enable inclusion listing of trusted domains, so they can communicate between iframes for openframe.</td>
</tr>
<tr>
<td>Requirement</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Medium) If you do not inclusion list intended domains, the ability to embed other pages within the Now Platform instances may be limited.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(High) If a web page contains event handlers that do not perform proper origin validation, a web page, or script from any origin, can communicate with it. It can also initiate any functionality performed by the event handler. Communication with iframes from other domains is a security risk.</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.

**URL allow list for logout redirects (instance security hardening)**

Use the `glide.security.url.whitelist` property to add extra layer of validation to ensure whether any external URL introduced should be a part of inclusion listed URLs.

Open redirection occurs when a vulnerable web page is redirected to an untrusted and malicious page that may compromise the user. Open redirection attacks come with a phishing attack because the modified vulnerable link is identical to the original site, increasing the likelihood of success for the phishing attack.

This property is applicable in the following cases:
   - `/logout.do?sysparm_goto_url={External URL}`
   - `/cms_login_redirect.do?sysparm_goto_url={External URL}`

Users are directed to an external trusted site after they log out of the instance:
   - `/logout_redirect.do?sysparm_url={External URL}`
   - `/saml_redirector.do?sysparm_uri={External URL}`

When SAML is enabled, it invokes an identity provider (IDP) logout URL.
More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.security.url.whitelist</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To implement safe URL redirect during login, logout, or other redirects. This property mitigates one of the OWASP top 10 attacks called Invalidated Redirects and forwards.</td>
</tr>
<tr>
<td>Type</td>
<td>String</td>
</tr>
<tr>
<td>Value</td>
<td>Your organization's approved URLs [Some Defined FQDN (Fully Qualified Domain Name) Ex. <a href="http://www.servicenow.com">http://www.servicenow.com</a>]</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Medium) This remediation enforces validation on logout page. It might have a functional impact on a user of an instance with an SSO/SAML configuration.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) Client-side open redirection can enable attacker to redirect victims/users to attacker-controlled website and is viewed as a security risk.</td>
</tr>
<tr>
<td>References</td>
<td>Multi-SSO (SAML 2.0) errors and fixes</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.

Virtual agent embedded client content security policy (instance security hardening)

Use the com.glide.cs.embed.csp_frame_ancestors property to enable the configuration of the frame-ancestors policy for only the https://<your-instance>.service-now.com/sn_va_web_client_app_embed.do page.

The Virtual Agent Plugin enables embedding of a client in an external web page. To enable the client page to be embedded in the web page, the Content Security Policy must allow the external page as a parent frame.

**Note:** Avoid using only '*' as the Content Security Policy because it would enable all domains and leave the application potentially vulnerable to clickjacking.

More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>com.glide.cs.embed.csp_frame_ancestors</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>No</td>
</tr>
<tr>
<td>Purpose</td>
<td>To enable creation of customized Content Security Policy for the embeddable Virtual Agent page.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>Set to trusted domains</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(High) Virtual Agent embeddable client doesn't allow itself to be embedded in external sites unless Content Security Policy is configured properly.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) If configured improperly (allowing all parent frames), it may possibly leave the embeddable client page vulnerable to clickjacking.</td>
</tr>
<tr>
<td>References</td>
<td>Embed the Virtual Agent web client in an external web page</td>
</tr>
<tr>
<td></td>
<td>To learn more about creating a frame-ancestors Content Security Policy, see here.</td>
</tr>
</tbody>
</table>

**Steps to configure**

1. Navigate to `/sys_properties_list.do`.
2. Search for the `com.glide.cs.embed.csp_frame_ancestors` property.
3. Assign acceptable content security policy (allow only company or other accepted domains), then click **Update**.

Virtual agent embedded client X-Frame-Options (instance security hardening)

Use the `com.glide.cs.embed.xframe_options` property to enable the configuration of the X-Frame header for only the `https://<your-instance>.service-now.com/sn_va_web_client_app_embed.do` page.
The Virtual Agent Plugin enables embedding of a client in an external web page. To enable the client page to be embedded in the web page, the X-Frame-Options header must enable the iframe to be included in the parent frame.

**Note:** Avoid using allow-from * as the X-Frame-Options header value because it would enable all domains and leave the application potentially vulnerable to clickjacking.

### More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>com.glide.cs.embed.xframe_options</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>No</td>
</tr>
<tr>
<td>Purpose</td>
<td>To enable specification of the directive for the X-Frame-Options header for the embeddable Virtual Agent page.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>Allowed from https://&lt;yourdomain&gt;.com</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(High) Virtual Agent embeddable client doesn't enable itself to be embedded in external sites unless X-Frame-Options header is configured properly.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) If configured improperly (allowing all parent frames), it may possibly leave the embeddable client page vulnerable to clickjacking.</td>
</tr>
<tr>
<td>References</td>
<td>Embed the Virtual Agent web client in an external web page</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see [Add a system property](#).

### X-Frame-Options: SAMEORIGIN (instance security hardening)

Use the `glide.set_x_frame_options` property to set the X-Frame-Options response header to SAMEORIGIN for all UI pages.

Use the X-Frame-Options HTTP response header to indicate whether browser should be allowed to render a page in a `<frame>` or `<iframe>`. Sites can use this function to avoid clickjacking attacks by ensuring that their content is not embedded into other sites.

### More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.set_x_frame_options</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To mitigate against ClickJacking attacks.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) This remediation enforces the restriction for rendering a Now Platform application in a third-party application in the form of an iFrame. If you have such an integration, the application wouldn't render in the customized third-party app.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) The Same Origin policy enables you to restrict a domain from retrieving a script or a resource from another domains. All modern browsers support this functionality.</td>
</tr>
<tr>
<td></td>
<td>The policy validates the connection based on protocol, port, and host. CORS (Cross Origin Request) is a modification to Same Origin Policy that enables access to resources/scripts from another domain when explicitly stated as a part of header value.</td>
</tr>
<tr>
<td></td>
<td>• In this case, the X-Frame-Options header controls whether the Now Platform application can be rendered on the third-party website.</td>
</tr>
<tr>
<td></td>
<td>• It reduces the sensitive exposure, because the property value, when set to <strong>SAMEORIGIN</strong> doesn't enable the rendering to happen.</td>
</tr>
</tbody>
</table>

### References

- Available system properties
- Configure iFrames
  - [https://community.servicenow.com/thread/170205](https://community.servicenow.com/thread/170205)
  - [https://community.servicenow.com/thread/177764](https://community.servicenow.com/thread/177764)

To learn more about adding or creating a system property, see [Add a system property](#).

### XML external entity processing validation

These properties enable entity expansion, and restrict any external entity (for example, URL) when included as a part of XML DOCTYPE reference. DTD is basically an XML schema. If you are looking for a solution for entity declarations that could have potential for XXE (external entity), enable an inclusion listed defense against XXE using system properties.

#### For XMLDocument and XMLUtil parsing

If your customizations use `XMLDocument` or `XMLUtil`, set the following system properties. They control entity expansion and enable the validation of external entities, which allow processing of only ones on inclusion lists.

**Setting entity expansion threshold (instance security hardening)**

Use the `glide.xmlutil.max_entity_expansion` property to change the maximum entity expansion limit to a smaller number.

The Now Platform doesn't process further entity expansions that are greater than the allowed limit specified in this property.

**Note:** 3000 is the default minimum imposed by the Now Platform, which is considered to be a safe threshold. Hence, platform considers this default minimum if the integer value you enter is below 3000.

### More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td><code>glide.xmlutil.max_entity_expansion</code></td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>This remediation control must be enabled to defend against XML Entity Expansion/Billion Laugh attack.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>3000</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) If the customization is using large entity expansion, then, the Now Platform might block further processing.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(High) An attacker can use this vulnerability to expand data exponentially, quickly consuming all system resources.</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.

XMLdoc/XMLUtil entity validation with allow list (instance security hardening)

Use the glide.xml.entity.whitelist.enabled property to enable the validation of external entity, and only allows processing of inclusion listed ones.

- If you set this property to **true**, it allows processing of only inclusion listed entities (recommended setting).
- If you set this property to **false**, it allows processing of all external entities.

**Prerequisites**

Before setting this property, define a listing of comma-delimited FQDN in the glide.xml.entity.whitelist property, which are the only URLs that can be reached using XML Entity processing. property. To learn more, see XML external entity processing - whitelist.

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.xml.entity.whitelist.enabled</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>This remediation control must be enabled to defend against XXE attacks.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) If the customization is using external entity, not inclusion listed in the glide.xml.entity.whitelist property, the Now Platform might block further processing. To learn more, see XML external entity processing - whitelist.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(High) An attacker can use the DTD to include arbitrary HTTP requests that the server might execute. This could lead to other attacks using the server's trust relationship with other entities.</td>
</tr>
<tr>
<td>Workaround</td>
<td>If you are not using external entity expansion, disable it. To learn more, see Disable entity expansion.</td>
</tr>
</tbody>
</table>
To learn more about adding or creating a system property, see Add a system property.

*For XMLDocument2 parsers*

If your customizations use a XMLDocument2 parser, use the following system properties to enable external entity validation.

Disable entity expansion (instance security hardening)

If customizations do not require entity expansion, use the `glide.stax.allow_entity_resolution` property to completely disable external entity expansion. The XML completes parsing but doesn't include any internal or external entities.

- If you set this property to `true`, all external entities attempt to resolve or expand subject entities, subject to the setting of the `glide.stax.whitelist_enabled` property.
- If you set that property to `true`, all entity resolution and expansion is blocked (recommended setting). To learn more, see XMLdoc2 entity validation with whitelist.

**Prerequisites**

Before setting this property:

- Set the `glide.xml.entity.whitelist.enabled` and `glide.stax.whitelist_enabled` properties to true. To learn more, see XMLdoc/XMLUtil entity validation with whitelist and XMLdoc2 entity validation with whitelist.
- Define a listing of comma-delimited FQDN in the `glide.xml.entity.whitelist` property, which are the only URLs that can be reached using XML Entity processing, property. To learn more, see XML external entity processing - whitelist.

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.stax.allow_entity_resolution</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>This remediation control must be enabled to defend against XML Entity Expansion/Billion Laugh attack.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>false</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) If the customization is using entity expansion, then, the Now Platform might block further processing.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(High) An attacker can use this vulnerability to expand data exponentially, quickly consuming all system resources.</td>
</tr>
<tr>
<td>Workaround</td>
<td>If the customization do require entity expansion, set this property to true and follow the steps documented in XMLdoc2 entity validation with whitelist.</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.

XMLdoc2 entity validation with allow list (instance security hardening)
Use the `glide.stax.whitelist_enabled` property to enable processing, using XMLDocument2, of external entities that are inclusion listed.

**Prerequisites**

Before setting this property:

- Set the `glide.xml.entity.whitelist_enabled` property to true. To learn more, see [XMLdoc/XMLUtil entity validation with whitelist](#).
- Define a listing of comma-delimited FQDN in the `glide.xml.entity.whitelist` property, which are the only URLs that can be reached using XML Entity processing. To learn more, see [XML external entity processing - whitelist](#).

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.stax.whitelist_enabled</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>This remediation control must be enabled to defend against XML External Entity attacks.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) If the customization is using an external entity that is not inclusion listed, the Now Platform might block further processing. To learn more, see <a href="#">XML external entity processing - whitelist</a>.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(High) An attacker can use the DTD may include arbitrary HTTP requests that the server may execute. Using the server's trust relationship with other entities, it could lead to other attacks.</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see [Add a system property](#).

**XML external entity processing - allow list (instance security hardening)**

Use the `glide.xml.entity.whitelist` property to enable access to a listing of comma-delimited FQDN, if needed. These URLs are the only ones that can be reached using XML Entity processing.

**Prerequisites**

Before setting this property, set the `glide.xml.entity.whitelist.enabled` property, which enables the validation of an external entity, and only allows processing of the inclusion list you specify in the `glide.xml.entity.whitelist` property. To learn more, see [XMLdoc/XMLUtil entity validation with whitelisting](#).

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.xml.entity.whitelist</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To create an inclusion list of URLs that XML Entity processing can access.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>User Specified (for example, <a href="https://google.com">https://google.com</a>)</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) External entity processing might be blocked if not mentioned in the inclusion list. When the inclusion list is enabled, it requires the PUBLIC form of an external entity definition.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(High) An attacker can use the DTD may include arbitrary HTTP requests that the server may execute. This could lead to other attacks using the server's trust relationship with other entities</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.

**Session management (instance security hardening)**

Session management helps to properly identify traffic that belongs to a specific user. Take precautions to ensure no abuse of the trust relationship.

Web applications can create sessions to track anonymous users after the first user request. An example would be maintaining the user language preference, ensuring:

- Identification of the user on any subsequent requests.
- Application of security access controls.
- Authorization of access to the user private data.
- Increase of the usability of the application.

Therefore, current web applications can provide session capabilities both pre and post-authentication.

**Authentication and Session Management**

Authentication is the process of verifying that an individual, entity, or website is who it claims to be.

Authentication attempts to verify the digital identity of the sender of a communication. Testing the authentication schema means understanding how the authentication process works, and using that information to circumvent the authentication mechanism. A common example is the log in process. Authentication takes place after submission of a user name, user ID, and one or more items of private information that only the user would know.

Session management includes security-related properties that an administrator can configure to ensure that secure session management mechanisms are established in the Now Platform.

**Absolute session timeout (instance security hardening)**

Use the `glide.ui.user_cookie.max_life_span_in_days` property to set a maximum cap for a valid user session to expire before forcing a user to reauthenticate into the instance.

It enables the user cookie to be valid for the duration of specified days, starting when the cookie was first issued. The default value is 30 days, and the maximum cap is at 365 days.
More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.ui.user_cookie.max_life_span_in_days</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To force the user to relogin after specific days.</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Medium) This property enforces mandatory relogin by avoiding any sort of cookie rotation after a given timeframe.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) The user cookies being active for an indefinite amount of time is a security risk and should expire on a time-based configuration.</td>
</tr>
<tr>
<td>References</td>
<td>Available system properties</td>
</tr>
<tr>
<td></td>
<td>Change settings for the Remember me check box and cookie</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see [Add a system property](#).

**Anti-CSRF token (instance security hardening)**

Use the `glide.security.use_csrf_token` property to ensure the use of a secure token to identify and validates incoming requests, which in turn are used to prevent these attacks.

Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they’re currently authenticated. CSRF attacks specifically target state-changing requests, not theft of data, since the attacker has no way to see the response to the forged request.

The following properties can be enabled for added controls over CSRF token:

- `glide.security.csrf_previous.time_limit`
- `glide.security.csrf_previous.allow`
- `glide.security.csrf.strict.validation.mode`

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.security.use_csrf_token</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To protect the application from potential CSRF attack.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) This remediation enables an extra validation step before the instance user submits a write request to the instance. Every write request contains a CSRF token (i.e a validation/CSRF ID tied to the user session). When the user session expires, the secure token expires with it.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Security risk</td>
<td>(High) Cross Site Request Forgery is a significant security risk that violates the integrity of the instance data. An attacker can launch the CSRF attack by abusing the trust of an instance user. With the help of social engineering attacks, a user can submit a malformed request on behalf of the attacker on the instance.</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.

**Change default credentials (instance security hardening)**

Use the **Password needs reset** check box in Users and Groups to ensure that an illegitimate user can't take advantage of default data.

The Now Platform includes some default data when the instance is zbooited, or when you provision a new instance. It might contain the demo user accounts like default admin, ITIL, and employee. Setting the property makes it necessary to change the default admin, ITIL, and employee credentials when logging in to the application.

**Steps to configure**

1. Log in with the username `admin` and the password `admin`.
2. Navigate to **System Security > Users > Users and Groups**.
3. Search for the user under User ID `admin` and Name `administrator`. Click the `admin` User ID to modify the user’s settings.
4. Modify the **Email** field to reflect a valid email address for that user.
5. Select the **Password needs reset** check box.
6. Click **Update**.
7. Log out and log in again. You are prompted to set a new password.

8. Repeat steps 3 through 7 for ITIL and employee accounts.

Cookies HTTP only (instance security hardening)

Use the `glide.cookies.http_only` property to enable the HTTPOnly attribute for sensitive cookies.

Use the HTTPOnly attribute to prevent attacks, such as cross-site scripting, because it doesn't allow access to the cookie using a client-side script, such as JavaScript. It does not eliminate cross site scripting risks but does eliminate some exploitation vectors.
### More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.cookies.http_only</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To mitigate the risk of client-side script accessing the protected cookie.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) This remediation adds an extra HTTPOnly flag in on session cookies, thus protecting them from being stolen.</td>
</tr>
<tr>
<td></td>
<td>• If you have custom functionality that requires JavaScript to access the user's cookie, it breaks that functionality. It should not be the case under normal circumstances.</td>
</tr>
<tr>
<td></td>
<td>• The Now Platform handles session management and there shouldn't be a reason for a custom script to access the user's cookies.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) Session cookies in the application authenticate an end user and provide implicit access permissions on the application. That means there is a need to secure them from being stolen or exported. HTTP Only flags protect the session cookies from JavaScript injections or cross site scripting vulnerabilities stealing them.</td>
</tr>
<tr>
<td>References</td>
<td>Available system properties</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.

### CSRF strict validation (instance security hardening)

Use the `glide.security.csrf.strict.validation.mode` property to enable CSRF token strict validation. If the CSRF token doesn't match, it prevents resubmission of the request.

### More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.security.csrf.strict.validation.mode</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To enforce strict validation of CSRF token, and prevents its reuse.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Medium) This remediation enables an extra validation step before the instance user submits a write request to the instance. It checks whether the current CSRF token has been used previously. If Yes, it prevents submission of further write requests.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) Cross site Request Forgery is a significant security risk that violates the integrity of the instance data. An attacker can launch the CSRF attack on any instance user by abusing the trust of the instance user. With the help of social engineering attacks, a user can submit a malformed request to the instance on behalf of the attacker.</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.

**Disable password-less authentication (instance security hardening)**

Use the glide.login.no_blank_password property to prevent users from logging in to the Now Platform with blank passwords, or by leaving the Password field empty.

Even if the admin purposefully assigns an empty value or blank password in user records, a user can't log in without providing a value in the Password field.

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.login.no_blank_password</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To ensure strong authentication as sometimes the username are easy to guess within an organization.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) Operations should not use blank passwords because it is viewed as a critical security risk. However, if there is a valid case for such usage, there is a possibility of an outage. Users with blank passwords wouldn't be able to log in to the instance.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(High) An attacker is able to log in to the instance with the default usernames, or by specific individual/group (usually firstname.lastname) without any password. Doing so is viewed as a critical security risk, because it would enable a public user to violate the confidentiality and integrity of the instance data.</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.

**Enable multi-factor authentication (MFA) (instance security hardening)**

Use the glide.authenticate.multifactor property to enable Multi-Factor Authentication (MFA) in the instance.

MFA is a security requirement that requires a user to enter more than one set of credentials to authenticate to an instance.

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.authenticate.multifactor</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>Strengthen instance security by introducing multi-factor authentication for interactive user logins.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Medium) Enabling this property improves the experience of the user. It acts as an extra layer of protection and security against compromised credentials.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) If this property is not enabled, there is a risk of unauthorized access to sensitive data.</td>
</tr>
<tr>
<td>References</td>
<td>Configure multifactor authentication (MFA)</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.

**Enforce strong passwords (instance security hardening)**

Use the `glide.enable.password_policy` property to enable password policy checks whenever a user changes their password using the user interface.

To define which password policy to use once this property is enabled, see Enable password policies on your instance.

**Note:** The `glide.enable.password_policy` does not apply when an administrator changes a password or adds a user through script.

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.enable.password_policy</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Purpose</td>
<td>To apply password policy at time of password change.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true (for higher strength passwords)</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Medium) Setting the property to true turns on password policy checks when a user resets their password.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) Without a password policy, a user can create a weak password which increases the likelihood of an adversary gaining access to the instance.</td>
</tr>
</tbody>
</table>

**Steps to configure**

If you configure this setting in the Hardening Compliance Configuration page in the Instance Security Center:

1. Under **Medium**, Select **Session Management**.
2. In the **Enable Password Reset Policy Check** setting, select **Medium** for medium strength passwords, or **Strong** for more robust, higher strength passwords. Selecting one of these options sets the `glide.enable.password_policy` property to true and starts a workflow that automatically updates your password policy.

Additionally, you can set the `glide.apply.password_policy.on_login` system property to enable password policy checks at the time of log in.

**Managing failed login attempts (instance security hardening)**

Two script actions are available that enable a site administrator to manage the number of times a user can provide an incorrect password before being locked out from the Now Platform. You can enable either of these script actions to manage failed login attempts.

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property/Plugin Name</td>
<td>N/A</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Policy &gt; Script Actions</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To enforce strict policy for failed login attempts to avoid brute forcing of credentials.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>Active</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) This remediation would enable administrator of the instance to monitor and report any malicious user access. No functionality impact, only User experience change.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) Apply a defined logging and auditing strategy so that you can identify and act on suspicious activity in a timely manner.</td>
</tr>
</tbody>
</table>

**Steps to configure**

1. Navigate to **System Policy > Script Actions**.
2. Search for the name **SNC User**.
3. To enable management of failed login attempts, change the Active state of either the **SNC User Lockout Check with Auto Unlock** or **SNC User Lockout Check** scripts actions from **false** to **true**.

![Script Actions](image)

4. To reset the failed login counter after a successful login, you can activate the **SNC User Clear** script action.

**Password field auto-complete (instance security hardening)**

Use the **glide.login.autocomplete** property to enable browsers to use auto-complete on password fields in login forms.

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.login.autocomplete</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To disable browser to attempt auto-complete for a password field.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>false</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) This remediation causes the Password field autocomplete flag to be turned off such that password history cache by browser is not shown in the field. There shouldn't be any functionality impact.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Low) User authentication fields should be validated and should never let the client-side caching to happen.</td>
</tr>
<tr>
<td>References</td>
<td><a href="https://support.servicenow.com/kb_view.do?sysparm_article=KB0563953">https://support.servicenow.com/kb_view.do?sysparm_article=KB0563953</a></td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.

**Remove credentials from welcome page (instance security hardening)**

Modify the default content on the Welcome page to remove the default credentials.

**Note:** Two How to Login records are part of the demo data for the CMS plugin. If you do not install the demo data for an instance, these records do not exist. In that case, the configuration is considered as Security Compliant as per the recommended security practices. To learn more, see Security best practices (instance security hardening).
Steps to configure

1. Navigate to System UI > Welcome Page Content >.
2. Find the two sections with a short description of How To login.
3. Change the Active state of each from true to false.

Remove remember me (instance security hardening)

Use the glide.ui.forgetme property to remove the Remember Me check box from the login page to prevent login information from being cached.

More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.ui.forgetme</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To ensure that no authentication information is cached.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) This remediation would change the user experience by automatically logging them out of the instance when their session expires. The session expiration would solely depend on the value set in the system property as detailed in Manage user sessions.</td>
</tr>
</tbody>
</table>
| Security risk                    | (Medium) When you select the Remember me check box at login, an extra cookie is stored on the user's computer.  
  • Its purpose is to automatically re-establish the session for the subsequent visits of the logged-in user.  
  • It poses a security risk as it allows the user session to be active until they deliberately log out. The likelihood of an attack for this scenario increases when the end user has left the browser unattended, or if it is compromised from a different attack. |
| References                       | Remove the Remember me check box                                           |

To learn more about adding or creating a system property, see Add a system property.

Rotate HTTP session identifiers (instance security hardening)

Use the glide.ui.rotate_sessions property to enable rotation of the HTTP session identifiers to reduce security vulnerabilities.

If an unauthenticated user's session ID doesn't change after authentication, a web application is vulnerable to a session fixation attack. A malicious user could start an unauthenticated session and give the associated session ID to the victim. Once the victim authenticates, the malicious user now shares that authenticated session.
More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.ui.rotate_sessions</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To achieve more secure session authentication.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Medium) This remediation modified the SessionID when user navigates from unauthenticated page to authenticated pages.</td>
</tr>
<tr>
<td></td>
<td>• If you are using a proxy or hardcoding the SessionID when a user first logs in, or for any purpose, then there can be a potential functionality impact.</td>
</tr>
<tr>
<td></td>
<td>• If you are using the SAML 2.0 plugin for Single Sign-on authentication, it might interfere with the session information sharing between the instance and the Identity Provider. In such case, you can set this property to false.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Late) SessionID is used to process and authenticate the instance user by maintaining the session state on the browser. Thus, SessionID is deemed as sensitive data and should be secure by default. Session Rotation is a security control that enforces the alteration of sessionID whenever the user navigates from unauthenticated pages to authenticate pages.</td>
</tr>
<tr>
<td>References</td>
<td>Authentication with SAML</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see [Add a system property](#).

**Secure session cookies (instance security hardening)**

Use the `glide.ui.secure_cookies` property to enforce the use of highly secure authentication cookies.

When you set the property to true, authentication cookies contain only a token, and have no embedded user information.

- On the service side, it looks up the token in the database, and associates it with a specific user. An authentication cookie can be used a single time only.
- Once used, the cookie is invalidated and removed from the database so that it can't be used again. The service then issues a new cookie.

More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.ui.secure_cookies</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To achieve more secure session authentication.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) When the property is set to true, pre-existing, low-security authentication cookies are rejected. When such a cookie is rejected, the user must login again.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(High) If you set the property to false, an attacker can exploit low-security authentication cookies, in an attempt to compromise the Now Platform.</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see [Add a system property](#).

**Security referral policy (instance security hardening)**

Use the `com.glide.security.referrerpolicy` property to control what referrer data should be sent in HTTP response headers when Now Platform pages sends requests for data. The Referrer-Policy value in an HTTP header controls what referrer information should be included with data requests.

**Security referral policy values**

Set the `com.glide.security.referrerpolicy` property to one of the following values.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Now Platform instance manages the level of information sent in referrer headers that is appropriate for the specific Now Platform page request.</td>
</tr>
<tr>
<td>same-origin</td>
<td>Now Platform pages send a full referrer URL within the instance and same domain, and no referrer header to outside origin.</td>
</tr>
<tr>
<td></td>
<td>This setting ensures a good level of instance security.</td>
</tr>
<tr>
<td>origin</td>
<td>Now Platform pages send the base URL in the referrer header within the instance and same domain, and also externally.</td>
</tr>
<tr>
<td></td>
<td>This setting ensures a good level of instance security.</td>
</tr>
<tr>
<td>origin-when-cross-origin</td>
<td>Now Platform pages send the whole URL in the referrer header within the instance and same domain, and send only the base URL externally.</td>
</tr>
<tr>
<td></td>
<td>This setting ensures a good level of instance security.</td>
</tr>
<tr>
<td>no-referrer-when-downgrade</td>
<td>Now Platform pages send the origin, path, and querystring in the URL, as long as there is no downgrade in a security protocol.</td>
</tr>
</tbody>
</table>

**Note:** This setting does not ensure a good level of instance security in the Now Platform and should not be used.
Referrer Policy example and values summary

![Browser window showing Headers with Referrer Policy set to no-referrer-when-downgrade]
More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>com.glide.security.referrerpolicy</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>No</td>
</tr>
<tr>
<td>Purpose</td>
<td>Controls how much incoming data is sent via the &quot;referrer&quot; header when a Now Platform page sends a request for data.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>default</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) If set to 'default', the Now Platform instance manages the level of information sent in referrer headers.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(High) Setting this property value to 'no-referrer-when-downgrade' does not ensure a good level of security for your instance.</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.

Session activity timeout (instance security hardening)

Use the glide.ui.session_timeout property to designate, in minutes, activity timeout value.

There are several functional impacts from setting this property:

- The longer the specified session time-out, the greater the amount of memory is utilized during a processing session. The base system uses a default Apache Tomcat timeout duration of 30 minutes.
- The Now Platform still logs out users out with Remember Me. After 30 minutes of inactivity in the application, the platform logs the user out automatically, unless the Remember Me check box in the login page is selected. What’s different is that they don’t log in again to continue.
- If there are gauges or content on users' home pages that refresh automatically, then this timeout may never be reached.

More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.ui.session_timeout</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To enforce session timeout.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>User specified timeout in minutes. 60 minutes is the recommended value, but this value may vary depending on functionality and security requirement. Do not set this value to more than one day.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Medium) This remediation enforces timely expiration of user account. No functionality impact, however User experience is altered.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) User sessions being active for indefinite amount of time is a security risk and should expire on a time-based configuration.</td>
</tr>
<tr>
<td>References</td>
<td>Manage user sessions</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see [Add a system property](#).

**Session window timeout (instance security hardening)**

Use the `glide.ui.user_cookie.life_span_in_days` property to set the expiration time period for the Remember Me cookie. The default value is 15 days and the maximum cap is at 30 days.

**More information**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td><code>glide.ui.user_cookie.life_span_in_days</code></td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>Yes</td>
</tr>
<tr>
<td>Purpose</td>
<td>To enable the default expiry of the 'remember me' cookie.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>User-defined integer value (# of days) [Example: 15]</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Medium) This property is enabled by the end user when the end user checks the Remember me check box from the login page and logs in to the Now Platform.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) The user cookies being active for an indefinite amount of time is a security risk and should expire on a time-based configuration.</td>
</tr>
<tr>
<td>References</td>
<td>Available system properties</td>
</tr>
<tr>
<td></td>
<td>Change settings for the Remember me check box and cookie</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see [Add a system property](#).

**Other settings and security resources**

This section contains security properties you set outside of the Instance Security Center, and also contains other security-related resources.

**Logging, auditing, and errors (instance security hardening)**

Apply a logging and auditing strategy so that you can identify and act on suspicious activity in a timely manner.

To learn more about what can be logged in the instance, see [System logs](#). Ensure that there is a schedule for monitoring system events such as login and failed logins by using **System Logs > Events**.

**Disabling SQL error messages (instance security hardening)**

Use the `glide.db.loguser` property to disable SQL error messages from rendering in a browser.
More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.db.loguser</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>No</td>
</tr>
<tr>
<td>Purpose</td>
<td>To disable SQL error messages from displaying within the browser.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>false</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) This remediation disables rendering of SQL error messages.</td>
</tr>
<tr>
<td></td>
<td>There is no impact to any functionality.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Medium) No sensitive SQL information that could help an attacker should</td>
</tr>
<tr>
<td></td>
<td>appear as a part of error message on a web page.</td>
</tr>
</tbody>
</table>

To learn more about adding or creating a system property, see Add a system property.

**MID server secure deployment guide (instance security hardening)**

The ServiceNow Management, Integration, and Discovery (MID) server is a lightweight Java application that runs as a Windows service or UNIX daemon on standard hardware, including virtual machines.

![MID server diagram](image)

It securely authenticates to your instance in the ServiceNow Cloud using its own login credentials, and facilitates the data transmission with your applications, data sources, and services. Multiple MID servers can be deployed in different network segments to provide additional scalability.

Consider the following factors regarding security for your MID Server:
Physical security
It is important to secure the physical hardware that hosts the MID Server or the hypervisor for virtualized MID Servers.

- Place the hardware in a secure location that protects the hardware from unauthorized access.
- Protect access to this location with an electronic card reader and CCTV monitoring.
- Place the physical hardware in a locked cage or a rack with physical key access control.

Virtual infrastructure security
Virtualization offers the flexibility to install multiple MID Servers in virtualized operating systems and networks in shared physical hardware.

Access to the hypervisor and virtual infrastructure management consoles must be protected to prevent unauthorized cloning of the virtualized MID Server:

- Limit the access to the hypervisor and virtual infrastructure management consoles by the trusted few admins.
- Only allow connections to the internal trusted network for management console such as ESX Server and VirtualCenter.
- Use VLANs to prevent network attacks.
- Follow the security guidelines published in the virtualization hardening guides from the vendors.

Operating system security
The MID Server stores its Now Platform username and password in its configuration file, named config.xml, for secure authentication to the instance.

The MID Server must be deployed in a secure and hardened operating system for protection against unauthorized access to the credentials:

- Limit the access to the operating system to a few, trusted administrators.
- Monitor the operating system logs to detect any unauthorized access, particularly attempts to access the config.xml file, as this file contains important MID Server configuration information.
- Install operating system security patches regularly with the latest anti-virus software and update AV definitions regularly.
- The MID Server requires a current Java framework to run. Keep Java updated regularly.
- Remove or disable unnecessary services and applications.
- Install an OS firewall to limit access to unauthorized ports.
- Follow the security guidelines published in the operating system hardening guides from the vendors.

Network security
The MID Server communicates on port 443 using SSL to the instance and requires no inbound connections.

To properly secure your MID server in a network, do the following:

- Install the MID Server on a secured server behind a corporate firewall for protection against unauthorized access from the internet.
- Configure the firewall on the MID Server to accept no inbound connections other than the ones required for corporate management of the operating system and hardware.
- The system that hosts the MID Server must be able to access the ServiceNow download site at install.servicenow.com.

Note: This URL is to the ServiceNow download site, which is not accessible from this topic.

The MID Serve host machine must be able to access that site to download the installer package. It contacts install.servicenow.com every 60 minutes to see if a newer version is available and if so, it performs an automatic upgrade. A MID Server upgrade also takes place when you upgrade an instance.

Firewall
Configure your firewall to allow outbound network traffic from the MID Server to your instance and auto-upgrade server.

To configure your firewall, use the following example syntaxes:

- `<source IP> TO <instance_name>.service-now.com ON PORT 443`
- `<source IP> TO install.service-now.com ON PORT 443`

**Administration and Management**

This section describes the security practices and guidelines for administering and managing the MID Server in your environment.

**Create an account with a mid_server role**

Create a user account in the instance that contains a mid_server role.

When you create a user account, follow these guidelines:

- Do not use an administrative account in the instance for the MID Server.
- Use sufficient password length and complexity for the MID Server account.
- The password should be at least 12 characters with upper, lower, numerical, and special characters.
- Use different MID Server accounts with unique passwords for different MID Servers in an instance.
- Use strict SOAP security feature to protect all tables with access control lists (ACL) by enabling **Enforce strict security on incoming SOAP requests** in System Properties > Web Services.
- Change the MID Server passwords at frequency that meets your organization's password policy.

**Note:** The Incompatible MID Server user role business rule prevents setting the Web Service access only option. To learn more, see the Create the MID Server user and grant the role.

**Setting up a MID server on a Windows host**

When you install the MID Server on a Windows host, it creates a Windows service. By default, this service is running as the local Windows system account. After the installation completes, change the newly created Windows service to an account with the least number of privileges required to run the MID Server on the Windows host.

1. Navigate to **Computer Management > Services and Applications > Services**.
2. Right-click **ServiceNow MID Server**, then click **Properties**.
3. Click the log in tab in the pop-up window.
4. Click the radio button next to **This account**.
5. Enter in the appropriate username and password of the account that the service should be running as:

![ServiceNow MID Server properties](image)

6. Click **OK**.

7. In the Services window, right-click **ServiceNow MID Server**, then click **Restart**.

8. Ensure that the MID Server was able to restart successfully and connect to the instance.

**Windows Discovery and Orchestration credentials**

Set up a local Windows or Active Directory account on the target systems with the least number of privileges necessary. It may not be necessary to use domain admin credentials.

The following product documentation pages provide guidance on the type of account that should be used and what permissions are required.

- Windows credentials
- Windows probes and permissions
- Microsoft Just Enough Administration (JEA) for Discovery

**Linux Discovery and Orchestration credentials**

Use a non-root account with limited pseudo-privileges on target Linux systems when performing discovery and orchestration.

Use the following guidelines:

- Use sufficient password length and complexity for the Linux account. The password should be at least 12 characters with upper, lower, numerical, and special characters.
- When configuring sudo permissions, local paths to binary executable files may differ depending on what Linux distro you are running, see **MID Server privileged commands**.

Encrypt MID server login credentials
By default, the MID Server login credentials are encrypted in the config.xml file.

When editing the config.xml file and supplying the password, ensure that the encrypt="true" attribute exists, using the following syntax:

```
<parameter name="MID.instance.username" value="MIDsrvadmin" />
<parameter name="MID.instance.password" encrypt="true" value="$ECUREpassw0rd" />
```

**Note:** Encrypting MID Server login Credentials does not substitute insecure server host with poor physical and network security. The password stored in the config.xml file is encrypted when you first start the MID Server, or, if it is an existing MID Server, on restart.

Set the minimum size of DH Group to 2048 bits
The National Standard Institute of Technology (NIST) disallowed the use of Diffie-Hellman (DH) 1024 bits key after year 2013. Set the minimum size of DH group to 2048 bits instead.

1. In the instance, navigate to **MID Server > Servers**.
2. Click the MID Server name that you would like to disable this functionality on.
3. In the MID Server configuration, click the **New** button next to Configuration Parameters.
4. In MID Server Configuration Parameter, configure the following parameter settings:
   - **Parameter name** mid.ssh.dh_group_length_min
   - **Value** 2048

Disable outbound SSL
You can disable SSLv2 and SSLv3 in the Now Platform. Setting this property forces the MID Server to use TLS, taking advantage of its increased security, when making outbound connections, such as REST and SOAP requests.

1. In the instance, navigate to **MID Server > Properties**.
2. Add a configuration parameter and set its value as follows:
   - **Name** glide.outbound.sslv3.disabled
   - **Value** true

Disable weaker algorithms
You can disable the weaker algorithms so that requests to any non-TLS 1.2 compliant HTTP server would fail where it used to work.

Edit the jre/lib/security/java.security file in the agent folder, using the following syntax:

```
jdk.tls.disabledAlgorithms=SSLv3, TLSv1, TLSv1.1, [other weak algos...]
```

**Note:** Keep in mind that this file is overwritten on upgrade, so you should have to have a process in place to reupdate this file after every upgrade.

### Revertible behavior

There are system properties that are categorized as either 'safe_overrides' or 'no_db_override'.

**Safe override**
The values for these properties can't be altered once changed (they are non-revertible).
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabling AJAXGlideRecord ACL checking (instance security hardening)</td>
<td>Access Control</td>
</tr>
<tr>
<td>Privacy on client-callable script includes (instance security hardening)</td>
<td>Access Control</td>
</tr>
<tr>
<td>Client generated scripts sandbox (instance security hardening)</td>
<td>Input validation (instance security hardening)</td>
</tr>
<tr>
<td>Collection mode override (deprecated)</td>
<td>Security inclusion listing (instance security hardening)</td>
</tr>
</tbody>
</table>

No DB override
The existing values for these properties can't be altered or overridden.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable file download restrictions (instance security hardening)</td>
<td>Attachments</td>
</tr>
</tbody>
</table>

Deprecated security properties
These security properties were deprecated in earlier releases.

Collection mode override (deprecated)
The `glide.whitelist.manager.collection_mode.override` property was designed to provide backwards compatibility for highly customized instances. It used package calls that were created on a version prior to Calgary and has since been deprecated.

More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td><code>glide.whitelist.manager.collection_mode.override</code></td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>No</td>
</tr>
<tr>
<td>Purpose</td>
<td>Disabling of the Collection Mode property closes the security gap that exists when importing Java package calls into an instance.</td>
</tr>
<tr>
<td>Recommended value</td>
<td>false</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(Low) There should be no impact as long as the results from the section 10.6 are reviewed and approved. To ensure proper functioning of the instance, test the changes in a non-production environment before deploying in the production environment</td>
</tr>
<tr>
<td>Security risk</td>
<td>(High) client-side API calls that result in data retrieval or object access on server are deemed to be dangerous from a security standpoint. Validate them for authorization and restriction for sensitive object access.</td>
</tr>
<tr>
<td>References</td>
<td><a href="https://support.servicenow.com/kb_view.do?sysparm_article=KB0621483">https://support.servicenow.com/kb_view.do?sysparm_article=KB0621483</a></td>
</tr>
</tbody>
</table>
SMTP authentication (deprecated)
The `glide.smtp.auth` property designated if an SMTP server should require username and password authentication entries.

### More information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property name</td>
<td>glide.smtp.auth</td>
</tr>
<tr>
<td>Configuration type</td>
<td>System Properties (/sys_properties_list.do)</td>
</tr>
<tr>
<td>Configure in Instance Security Center</td>
<td>No</td>
</tr>
<tr>
<td>Purpose</td>
<td>Enforces SMTP Authentication</td>
</tr>
<tr>
<td>Recommended value</td>
<td>true</td>
</tr>
<tr>
<td>Functional impact</td>
<td>(High) This remediation enforces authentication to the external mail server before the content is delivered in the form of an email. If automation is set up to deliver email content, there may be an impact until you set the property and provide a relevant username/password for mail server access.</td>
</tr>
<tr>
<td>Security risk</td>
<td>(Low) Enable SMTP authentication before sending the content to the external mail server. Authentication should always take place before the transactions take place to/from to the instance.</td>
</tr>
<tr>
<td>References</td>
<td>Email properties</td>
</tr>
</tbody>
</table>

### Other security hardening resources

The following are additional sources of information about security controls hardening, as it relates to the Now Platform.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Test Portal</td>
<td>Security Services Portfolio on HI</td>
</tr>
<tr>
<td>KB0538598</td>
<td>Customer Application Penetration Testing</td>
</tr>
<tr>
<td>KB0546756</td>
<td>Disabling public Content Management System (CMS) access</td>
</tr>
<tr>
<td>KB0550071</td>
<td>ServiceNow, Inc. instance access control review</td>
</tr>
<tr>
<td>KB0550613</td>
<td>Identifying and enabling IP address restrictions</td>
</tr>
<tr>
<td>KB0550828</td>
<td>Audit and review GlideAjax transactions</td>
</tr>
<tr>
<td>KB0550837</td>
<td>Script sandboxing remediation</td>
</tr>
<tr>
<td>KB0551031</td>
<td>Security remediation for password reset UI</td>
</tr>
<tr>
<td>KB0552835</td>
<td>Remediation for Demo User Accounts</td>
</tr>
<tr>
<td>KB0529232</td>
<td>ServiceNow, Inc. Monitoring - Overview and Insight</td>
</tr>
<tr>
<td>KB0564232</td>
<td>Using ServiceNow, Inc. mobile app with external authentication</td>
</tr>
<tr>
<td>Security &amp; Risk</td>
<td>ServiceNow, Inc. Community</td>
</tr>
</tbody>
</table>
**Instance Security Center**

Monitor the compliance level of instance security controls, view security event monitoring metrics, and configure and maintain instance security settings all from within the Instance Security Center. The Instance Security Center consolidates several key security components into a single control console that helps you detect, protect, and respond to instance-based security events.

From the Instance Security Center homepage, you can view the security compliance score for your instance and monitor its overall security health. You can then configure or update system properties that are related to your instance security so that they comply with security requirements.

**Note:** The Instance Security Center does not support domain separation.

### User roles

To use the Instance Security Center, you must have the admin or security_dashboard_user role.

<table>
<thead>
<tr>
<th>User</th>
<th>Required role</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security personnel in your organization who monitor security-related information for an instance and have authorization to change security hardening settings. They should be able to return to the Instance Security Center at any time to adjust settings and manage the overall security health of an instance.</td>
<td>admin</td>
<td>Continually monitor and manage instance security compliance.</td>
</tr>
<tr>
<td>Security personnel in your organization who monitor security-related information for an instance but do not have authorization to change security hardening settings. For example, a security analyst with this role can view instance security information. However, another user with an admin role would have to make actual security setting updates.</td>
<td>security_dashboard_user</td>
<td>Continually monitor instance security compliance to detect and respond to security threats.</td>
</tr>
</tbody>
</table>

**Warning:** To ensure that the Instance Security Center receives up-to-date security information with every upgrade, do not customize this module. If you change any security settings on your instance, make sure that you test them in a non-production environment first.

### Instance Security Center components

To access the Instance Security Center, navigate to System Security > Instance Security Center or the System Administration homepage.
Configure Security Notifications
Starting in Paris, ISC users can now subscribe to security email notifications. Begin updating by selecting

Hardening: Live Protection
Access restrictions help reduce the attack surface and the likelihood of malicious actions on your system. A new rule has been added to defend against unauthorised access.

Failed Logins
Real-time: 10:48
19

External Logins
Real-time: 10:48
0

Trusted Incoming Email
Real-time: 10:48
0

Daily Compliance Score
83%
The Instance Security Center homepage contains the following security components:

- Administrator messages
- Rotating security banner
- Search
- Security event ribbon
- Daily compliance score
- Session Management
- Hardening
- Auditor
- Metrics (user, email, and antivirus)
- Resources
- Security notifications
- Tours
- Security testing portal
- Security center
- Help
- Virtual Agent access

**Administrator messages**

Messages and reminders, intended mostly for administrators, appear above the rotating security banner.

- For example, a Configure Security Notifications message appears that reminds administrators to configure preferences for security notifications if they have not done so already. It also points them to the proper page to do so.
- To learn more about security notifications and enabling notification preferences, see Security notifications.

**Note:** The administrator messages banner does not appear for non-admin users, or if there are no actionable items for admin users.

**Rotating security banner**

To assist you in monitoring the security health of your instance, critical instance security messages appear in the rotating banner.

- Two to three security messages normally rotate at a regular interval.
- The dots at the bottom of the banner show you the total number of current security messages.
- To navigate through them, click the dots, or click the arrows that appear on either side of the messages.

The banner background colors indicate the relative severity of the messages.

<table>
<thead>
<tr>
<th>Color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red</td>
<td>Critical security situation requiring a timely response, or a recommendation on how to protect or respond to critical security events.</td>
</tr>
<tr>
<td>Dark gray</td>
<td>Non-critical warning message.</td>
</tr>
<tr>
<td>Blue</td>
<td>General information message.</td>
</tr>
</tbody>
</table>
To collapse or minimize the text content in the banner, click [icon]. To maximize the text content, click it again.

- When you use the Instance Security Center again, the text content appeared as collapsed or expanded, depending on how you used it during your previous session.
- If the text content itself changes, it appears as maximized for all users.

**Search**

Use the search bar to search the entire Instance Security Center for security resources that assist you with understanding and resolving security issues. You can search the following security-related resources:

- Now Support Knowledge Base articles
- Instance Security Center pages
- External Now Support links
- PA security widgets, such as the Daily Compliance Score and External Incoming Emails
- Banner content

**Event ribbon**

Use the event ribbon to view key security event monitoring metrics for the current instance.

- To manually scroll through the metrics, click the right or left arrow keys.
- To configure the event ribbon, click **Edit**.

To learn more about the event ribbon and how to configure it, see Monitor security events and Configure the security event ribbon.

**Daily compliance score**

The Daily Compliance Score section contains the **Daily Compliance Score**, **Session Management**, **Hardening**, **Auditor**, and **Resources** tiles.

You use the Daily Compliance Score to gauge how healthy your instance is from a security standpoint.

The Daily Compliance Score is a percentage score. It is based on how compliant the current settings of your instance security properties are with the compliance values published in the Instance Security Hardening Settings.

- To learn more about Daily Compliance Score calculations, and how hardening settings impact it, see Check the daily compliance score and configure security property settings.
- The **Refresh** button enables an administrator to instantly recalculate the Daily Compliance Score. To learn more, see How Daily Compliance score, trend, and graph data is refreshed.

**Hardening**

Use this process to adjust the specific security configuration properties that affect the Daily Compliance Score:

1. To access the Hardening Compliance Configurations page and perform instance security hardening, click the **Daily Compliance Score** tile or the **Hardening** link.

2. Specify if you want to view all or only recommended security controls, and then select the category you want to work in.
3. Set each security configuration property in the selected category. Click More Info to view detailed information for a property.

To learn more about hardening and optimizing security configuration properties to further increase compliance, see Adjust instance security settings to increase compliance.

To learn more about how trend and graph data is refreshed, see How Daily Compliance score, trend, and graph data is refreshed.

**Auditor**

Run the Auditor to scan your instance and find incorrect security definitions. It provides findings you can correct to help improve the security posture of your instance.

To access the Auditor page, click the Auditor tile or the Auditor link. To learn more, see Scan for incorrect security definitions.

**Session management**

Use Session Management to:

- View and manage user login sessions.
- See all users who are currently logged in to the instance.
- See detailed information about each session, such as the user name and IP address.
- Isolate and lock out specific user sessions that pose security risks.

To access the Session Management page, click the Session Management tile or link.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| User  | Name of the user associated with this login session.  

- To locate a specific user session, click the spotlight search icon ( ) to search by user, user agent keyword, or IP address.  
For example, if you want to find all current logins from a specific type of browser, enter the browser name as a keyword into the User Agent field.  
- Click a user name to access the user profile record. You can modify the user profile only if you have an assigned admin role.  

**Note:** To learn more about user profiles, see Create a user. |
| MFA   | Check box indicating if Multifactor Authentication (MFA) is enabled for the logged in user. To learn more about MFA, see Multifactor authentication (MFA). |
| Active| Check box indicating if the logged in user is active or inactive. |
### Field

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Agent</td>
<td>Type of browser and the device operating system for the user login session.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the logged in user.</td>
</tr>
<tr>
<td>Last Accessed</td>
<td>Date and time this user session last accessed the instance.</td>
</tr>
</tbody>
</table>

**Note:** To view detailed information for a particular login session, or to lock out the session itself, click the User Agent, IP Address, or Last Accessed fields.

### Metrics (user, email, and antivirus)

View detail for the following types of metrics:

<table>
<thead>
<tr>
<th>Type of metric</th>
<th>Description</th>
</tr>
</thead>
</table>
| User | Security metrics that are associated with user activity in the instance.  
To access the User Metrics page, click the Metrics link, and then select User Metrics. |
| Email | Security metrics that are associated with user activity in the instance.  
To access the User Metrics page, click the Metrics link, and then select User Metrics. |
| Antivirus | Security metrics that are associated with antivirus event activity in the instance.  
To access the Antivirus Metrics page, click the Antivirus tile or click the Metrics link, and then select Antivirus. |

**Note:** To learn more about monitoring each type of metric, see Monitor user, email, and antivirus metrics.

### Resources

Access Now Support Knowledge Base articles, resources, and blogs that are related to instance security. These resources include security settings, coding, compliance, fixes, and related topics. To access the Resources page:

1. Click the Resources tile or link.
2. In the Resources page, click a category:

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
</table>
Security notifications

A notifications bell icon appears in the Instance Security Center, with a count total of unread security notifications. Notifications persist and are included in this count until you mark them as read.

1. Click the bell icon to view the first five unread security notifications.

   A notification appears when Admin Login, Admin Unlocked, Failed Login, High Privilege Role, Impersonation, Security Elevation, and Weekly Digest events take place in your instance. To learn more about these security events, see Monitor security events.

2. To view detailed information for a specific security event, click the notification.

   For example, if you click a High Privilege Role notification, you can view the Roles (sys_user_role) table. Use this table to see which users were assigned privileged roles during the calendar day. Using this history helps you to determine if roles have been properly assigned.

3. If there are more than five unread notifications, click View All Notifications to access an All Notifications page with a listing of all unread notifications.

   • To view detailed information for a specific security event, click the notification.
   • To mark all listed notifications as read, click Mark All as Read.

Note: As an administrator, you can also configure preferences for sending specific types of notifications for each type of security event. To learn more, see Set preferences for security event notifications.

Tours

Click the Tours link to view a guided visual tour of the Instance Security Center.

• The guided tour includes only the security monitoring functions that are listed on the homepage.
• It does not include the security functions that you access when you click the tiles or links on the homepage.

Security testing portal, security center, and help

The Now Support Service Portal is a central resource that you use to manage instances, tasks, and accounts. You can also access useful resources you can use to diagnose and resolve security and technical issues in your instance.

To access these resources, click Learn More or Get Help in the following tiles:
### Security Testing Portal

### Security Center

### Help
Access to the following help resources in the Now Support Security Portal:
- Ask an expert to find answers to common questions.
- Report an issue or outage to ServiceNow Global Technical Support by opening a case.
- Self-Service Support Resources, including:
  - Videos
  - Documentation
  - Now Community
  - Knowledge Base
  - Known Error Portal
  - Security RFX Database
- Now Community questions that are recommended for your use.

### Virtual Agent access
The Virtual Agent is a platform for providing user assistance through conversations within a messaging interface.

If you have an assigned admin role and have activated the proper plugins, you can access the Virtual Agent and Natural Language Understanding (NLU) functions by clicking the Virtual Agent icon:

It enables you to perform the following tasks:
- Ask security-related questions, then get quick summary answers and reference links to learn more.
- Get answers related to the Instance Security Center, Platform Security, ServiceNow security policies, trust, governance, risk, and other processes.
- Search for security-related resources, such as Knowledge Base topics in the Now Support Security Portal.

**Note:** To learn more about how to use and activate the Virtual Agent, see:
- Virtual Agent
- Activate the ISC Virtual Agent interface

### Monitor security events
Analyze the event metrics in your instance so that you can identify and prevent potential security events.

In the event ribbon, which is on the Instance Security homepage, you can analyze these metrics and accompanying detail to identify potential security events in the instance.

- For each event metric, a real-time single score count appears, indicating how many times that the event occurred during the day in this instance. These single score reports are updated automatically as the corresponding events take place.
• Each event metric also contains compliance trend and graph information over a range of dates. This information updates on a daily basis when you run the performance analytics job. To learn more, see the Analyzing event trend detail section.

Event types

You can monitor at least six of the following types of events. For more than six events, use the left or right arrows below the event ribbon to scroll through them. To learn how to configure the event ribbon, see Configure the security event ribbon.

<table>
<thead>
<tr>
<th>Notification preference</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Logins</td>
<td>Number of login attempts in this instance, during the calendar day, by users who have an assigned admin role.</td>
</tr>
<tr>
<td>Admin Users Added</td>
<td>Number of users with an admin role that were added in this instance during the calendar day. For example, your instance may have a security issue if the count is 10, but 4 users are known to have an assigned admin role.</td>
</tr>
<tr>
<td>External Incoming Email</td>
<td>To learn more, see Email metrics.</td>
</tr>
<tr>
<td>External Logins</td>
<td>Number of users with an assigned snc_external role who logged into this instance during the calendar day. These logins typically occur for maintenance, support, consulting, or audit purposes. Monitoring this metric enables you to verify that the external login attempts are legitimate and not potential security issues. To learn more about assigning external user roles, see Explicit Roles.</td>
</tr>
<tr>
<td>Failed Logins</td>
<td>Number of attempted logins that failed in this instance during the calendar day. This metric may indicate that attempts are being made to log in and compromise your instance security.</td>
</tr>
<tr>
<td>Impersonations</td>
<td>Number of impersonation logins in this instance during the calendar day. To learn about impersonating users, see .</td>
</tr>
<tr>
<td>Quarantined Files</td>
<td>Number of files that were quarantined when you ran Antivirus Scanning in this instance during the calendar day. To learn more about quarantined files and Antivirus Scanning, see Antivirus metrics and Antivirus Scanning.</td>
</tr>
</tbody>
</table>
## Notification preference

<table>
<thead>
<tr>
<th>Notification preference</th>
<th>Description</th>
</tr>
</thead>
</table>
| Security Elevations     | Number of times that a security administrator has elevated security for standard users by changing their assigned user role to a high privilege security role during the calendar day. These high privilege security roles include oauth_admin, admin, security_admin, and impersonator.  
- This metric indicates that someone might have tried to elevate the security of an unauthorized user. Do not use this metric by itself to detect a specific security compromise. Instead, treat this metric as an indication that you should check another metric to see if a security compromise has occurred.  
- To learn more about elevating user security, see Elevate to a privileged role and Elevated privilege roles. |
| SNC Logins              | Number of Customer Service and Support personnel who logged into this instance using the hi-hopping technique during the calendar day. These logins typically occur for maintenance, support, consulting, or audit purposes.  
For information on how to control ServiceNow corporate employee access, see ServiceNow access control. |
| Spam                    | To learn more, see Email metrics. |
| Trusted Incoming Email   | To learn more, see Email metrics. |
| Untrusted Incoming Email | To learn more, see Email metrics. |
| Virus Types             | Number of different types of antivirus events that occurred in this instance during the calendar day. To learn more about antivirus event types, see . |

### Analyzing event trend detail

To view trend details for an event metric, click the event count to access the Analytics Hub page. The details that appear for the instance depend on the type of metric.

For example, to view a listing of each failed attempt on the Security Dashboard Event Logs page:

- Select the **Failed Logins** metric,
- In the Analytics Hub page, click **Show Records**.
- Click one of the failed login attempts.
- The detail includes the name of the user who attempted to log in, their IP address, and the table name that they tried to access.

You can set up event threshold triggers in the to provide alerts when a certain event occurs within a range of scores for an indicator. You can also set targets that enable you to visualize the difference between the desired score and the actual score of an event.
For example, you can set a threshold of 10 for the Failed Logins metric. When ten or more failed login attempts occur during the day, an alert is sent to specific security personnel. You can also set a similar target that provides a visual highlight in the Analytics Hub when 10 failed logins occur during a day.

Trend data and graphs that appear in Event ribbon tile and the Analytics Hub are updated after the performance analytics job executes at 02:00 local time. To learn more, see How Daily Compliance score, trend, and graph data is refreshed.

Configure the security event ribbon

Configure the security event ribbon on the Instance Security Center homepage to include only those events that are relevant for tracking instance security in your operations. You can also change the order in which the security event tiles appear on the ribbon.

Role required: security_dashboard_user or admin

The security event ribbon is initially populated with a full set of standard security events. You can customize it by removing the events that are not relevant to your organization.

- For example, if you suspect that security issues are due to the actions of internal personnel, include the Admin Logins, Admin Users added, and Security Elevations event indicators.
- These indicators monitor how many times users with admin roles attempted to log in and, if admin users were added, what attempts were made to elevate security roles.

Note: To learn about the types of security events that appear in the event ribbon, see Monitor security events.

2. In the event ribbon, click Edit

On the Edit Events form, the Selected column contains the events that are already listed.

3. To add security events to the event ribbon, move them from the Available column to the Selected column.
   To change the order the events appear on the ribbon, select an event, then click the up or down arrow to move it to its correct position.
   - Place the events in the same sequential order they should appear on the Instance Security Center event ribbon.
   - The events you place at the top of the Available column appear sequentially, beginning on the left side of the Instance Security Center event ribbon. The events placed towards the bottom of the column appear on to the right on the event ribbon.

4. To remove security events from the event ribbon:
   - In the Selected column, select the security events that you want to remove from the event ribbon.
   - Move them from the Selected column to the Available column.

5. Click Save.

Set preferences for security event notifications

Configure preferences for the types of notifications you want to receive for occurrences of specific security events. For each type, you designate whether to receive notifications by email, by push notification in Now Mobile, or in third party messaging applications such as Slack or Microsoft Teams.
To enable third party messaging applications to send security event notifications, you must activate the Messaging Notification (com.glide.notification.messaging) plugin. Individual users must configure their own settings. For details, see Notifications in messaging applications.

Role required: admin

1. In the Instance Security Center home page, click the profile menu, then click **Notification Preferences**.

<table>
<thead>
<tr>
<th>Notification preference</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Login</td>
<td>Send the selected type of notification whenever other users with assigned admin roles log into this instance from a different IP address.</td>
</tr>
<tr>
<td>Admin Unlock</td>
<td>Send the selected type of notification whenever an account for a high privilege user has been unlocked.</td>
</tr>
<tr>
<td>Failed Login</td>
<td>Send the selected type of notification whenever other users fail to log in into this instance in less than the number of attempts defined in the <code>glide.user.max_unlock_attempts</code> property. If you don't configure this property, the default value is 5. To learn more about this property, see Specify lockout for failed login attempts.</td>
</tr>
<tr>
<td>HP Role Added</td>
<td>Send the selected type of notification whenever a high privilege security role (including oauth_admin, admin, security_admin, and impersonator roles) is granted to another user. To learn more about elevating user security, see Elevate to a privileged role and Elevated privilege roles.</td>
</tr>
<tr>
<td>Impersonation</td>
<td>Send the selected type of notification whenever another user is impersonating you. To learn more about impersonating users, see Impersonate a user.</td>
</tr>
<tr>
<td>Security Elevation</td>
<td>Send the selected type of notification whenever other users are elevated to a security admin role in this instance.</td>
</tr>
</tbody>
</table>
| Weekly Digest | Send a weekly digest on the selected type of notification. It includes:  
  - A summary all security activities that took place in this instance throughout the week.  
  - The current daily compliance score for the instance. |

2. For each type of security event, select the appropriate check boxes to designate the type of notifications to send you. You can select multiple notification methods for each.

<table>
<thead>
<tr>
<th>Check box</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Send an email for this type of security event.</td>
</tr>
<tr>
<td>Check box</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Slack</td>
<td>Send notifications for this type of security event through Slack.</td>
</tr>
<tr>
<td><strong>Note</strong>: This column appears only if you have set up Slack integration to the Now Platform.</td>
<td></td>
</tr>
<tr>
<td>Teams</td>
<td>Send notifications for this security event through Microsoft Teams.</td>
</tr>
<tr>
<td><strong>Note</strong>: This column appears only if you have set up Microsoft Teams integration to the Now Platform.</td>
<td></td>
</tr>
<tr>
<td>Push</td>
<td>Send push notifications on Now Mobile for this type of security event.</td>
</tr>
<tr>
<td><strong>Note</strong>: This column appears only if you first log into Now Mobile.</td>
<td></td>
</tr>
<tr>
<td>Select All</td>
<td>Select a specific type of notification for all types security events. For example, click Select All located above Email if you want to receive email notifications for each security event type.</td>
</tr>
</tbody>
</table>

3. Click **Save**.

### Check the daily compliance score and configure security property settings

Review the Daily Compliance Score metric and security configuration properties to see if your instance complies with the suggested security requirements. You can affect the daily compliance score by updating non-compliant security properties in the Hardening Compliance Configurations page.

The Daily Compliance Score is a percentage score. It is based on how compliant the current settings of your instance security properties are with the compliance values published in the Instance Security Hardening Settings.

Review the daily compliance score of your instance regularly. Follow these guidelines when you are evaluating your daily compliance score:

- Greater than or equal to 90% indicates that the instance is compliant with critical security controls.
- Greater than or equal to 50% and less than 90% indicates a moderate level of security compliance.
- Less than 50% indicates a low level of security compliance.

### Adjust instance security settings to increase compliance

Using the Hardening Compliance Configuration page, harden and optimize non-compliant security properties that affect the daily compliance score of your instance. Its use ensures that your instance complies with the published security hardening standards, while fulfilling your company's security requirements.

Refer to the Instance Security Hardening Settings content for detailed descriptions, and compliance values, for the security-related system properties and plugins in the .

- Consult the Instance Security Hardening Settings whenever you set or update security-related properties, even if some of the compliance values may not be suitable for your instance.
When you are updating these properties, ensure that the instance continues to behave as expected. Consult with the appropriate internal personnel who have the expertise to determine the security impacts.

Role required: security_dashboard_user or admin

**Note:** If you have an admin role, you can view and edit security controls. If you have a security_dashboard_user role, you can view security controls, but you cannot edit them.

1. Navigate to **System Security > Instance Security Center**.
2. Click the **Daily Compliance Score** tile or the **Hardening** link to access the Hardening Compliance Configuration page.
3. In the Hardening Compliance chart, view the statistics for compliant and non-compliant security configuration properties.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant</td>
<td>Number of security configuration properties that comply with the compliance values in the Instance Security Hardening Settings.</td>
</tr>
</tbody>
</table>

**Note:** You cannot change the settings for compliant security properties in the Hardening Compliance Configuration. If you want to do so, you must update them in System Properties. To learn more, see Add a system property.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-Compliant</td>
<td>Number of security configuration properties that do not comply with the compliance values in the Instance Security Hardening Settings. You can update settings for non-compliant properties.</td>
</tr>
</tbody>
</table>

**Note:** To view the number of compliant or non-compliant security scores over a range of dates, move the blue dot on the slider below the Daily Compliance Score.

4. In **Show**, specify whether you want to access all security configuration properties, or only recommended ones.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>(Default) All compliant and non-compliant security configuration properties in each selected category.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recommended</td>
<td>Only recommended security configuration properties appear in each selected category. These security configuration properties are a selected subset of the most critical ones used to secure the Now Platform. Consider these security configuration properties to be the bare minimum number of settings you must set to secure the Now Platform.</td>
</tr>
</tbody>
</table>

**Note:** To fully secure your instance, use the **All** option. It includes all recommended security configuration properties too.
5. In **Categories**, select the category that contains the security configuration properties you would like to access:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>Access controls determine whether to grant or deny user access to a particular resource based on who is permitted to use those resources. To learn more, see <a href="instance_security_hardening">Access control (instance security hardening)</a> in the Instance Security Hardening Settings.</td>
</tr>
<tr>
<td>Attachments</td>
<td>Attachment security controls enable validation of incoming attachments to protect your instance against malicious files sent by attackers. To learn more, see <a href="instance_security_hardening">Attachments (instance security hardening)</a> in the Instance Security Hardening Settings.</td>
</tr>
<tr>
<td>Email Security</td>
<td>Email security encompasses security configuration properties an administrator can configure to ensure that proper security policies are in place for all inbound emails. To learn more, see <a href="instance_security_hardening">Email security (instance security hardening)</a> in the Instance Security Hardening Settings.</td>
</tr>
<tr>
<td>Input Validation</td>
<td>Input validation includes security-related properties that an administrator can configure to minimize entry of malformed data, regardless of source. To learn more, see <a href="instance_security_hardening">Input validation (instance security hardening)</a> in the Instance Security Hardening Settings.</td>
</tr>
<tr>
<td>Secure communications</td>
<td>Secure communications properties are those that an administrator can configure to secure the transportation of HTTP traffic. To learn more, see <a href="instance_security_hardening">Secure communications (instance security hardening)</a> in the Instance Security Hardening Settings.</td>
</tr>
<tr>
<td>Security Best Practices</td>
<td>Security best practices encompass security tasks that an administrator should perform periodically, within a certain interval of time, and include related configuration properties. To learn more, see <a href="instance_security_hardening">Security best practices (instance security hardening)</a> in the Instance Security Hardening Settings.</td>
</tr>
<tr>
<td>Security Inclusion Listing</td>
<td>Security inclusion listing includes security-related properties that an administrator can configure to restrict behavior to known inclusion listings. To learn more, see <a href="instance_security_hardening">Security inclusion listing (instance security hardening)</a> in the Instance Security Hardening Settings.</td>
</tr>
<tr>
<td>Session Management</td>
<td>Session management includes security-related properties that an administrator can configure to ensure secure session management in the . To learn more, see <a href="instance_security_hardening">Session management (instance security hardening)</a> in the Instance Security Hardening Settings.</td>
</tr>
</tbody>
</table>

6. Configure the non-compliant security properties in the selected category.

   - Unless otherwise specified, sliding the switch on sets a security property to its recommended setting. For example, you set most controls to true or false, but some require entry of a value, or values, such as a comma-separated value list.
   - To access the dedicated Instance Security Hardening Settings topic for the security control, and learn more about it, click **More Info**.

The Daily Compliance score increases or decreases depending on the changes that you make to the non-compliant security control settings.
How Daily Compliance score, trend, and graph data is refreshed

Trend and graph data in the Instance Security Center is updated after the performance analytics job executes at 02:00 local time. It appears in the Daily Compliance Score tile, in the Event ribbon tiles, and in the Analytics Hub page detail when you click one of the event tiles.

The [AppSec] Daily Data Management job is a regularly scheduled job that runs nightly and performs the following tasks:

1. Verifies if valid users have been assigned to the [AppSec] Daily Data Management and [PA AppSec] Daily Data Collection jobs when you first schedule them.
   - If you entered a valid user into the Run As field, the job continues processing. A valid user is one that is not locked out of the instance and has an assigned admin role.
   - If you entered an invalid user, an error message appears above the rotating security banner in the Instance Security Center.

   **Note:** To learn more about updating the assigned user when running scheduled jobs, see Create or schedule a data collection job.

2. Executes business logic to set the compliance state for the security properties you configure in the Hardening Compliance Configuration page. To learn more, see Check the daily compliance score and configure security property settings.

3. Runs the [PA AppSec] Daily Data Collection performance analytics job to collect compliance data and update the Daily Compliance Score.

Manually refreshing the Daily Compliance Score

Alternately, if you have an assigned admin role, you can refresh and recalculate the Daily Compliance Score at any time by clicking Refresh.

- The Refresh function performs the same tasks as the Daily Data Collection performance analytics job but does it in real time, rather than in a batch process.
- You typically use it when you want to perform updates to the Daily Compliance Score to immediately view the impact of instance security activities.
- There may be a slight delay before the updated score appears.

**Note:** The Refresh button does not appear for users with an assigned security_dashboard_user role.

**Note:** When you perform an upgrade (for example, from London to Quebec), the Instance Security Center (ISC) plugin is automatically activated. A ServiceNow-supplied fix script automatically assigns a custom user without any assigned roles.

Scan for incorrect security definitions

Run the Auditor to scan your instance and find incorrect security definitions. It provides findings you can correct to help improve the security posture of your instance.

The Auditor performs a “full-body” assessment of your instance health that analyzes your system configuration. For security scans, it compares your current security configuration to best practice definitions, and to security property compliance values.
From an instance security standpoint, it provides insights and recommendations into what you should continue doing, and where you might be able to improve. These insights and recommendations help you answer the following questions:

- Are the appropriate security-related properties set?
- Is the High Security plugin enabled?
- Do the right access control rules exist?

### Run the Auditor and analyze scan results

1. To run the Auditor, click **Audit** on the Instance Security Center home page.
2. When it completes, open Scan Results to review and analyze the security findings.
3. To review the detail for a specific scan result, double-click the result number. This information includes its status, scan type, execution time, and error messages.
4. Each of the Auditor findings contains resolution details, and a URL to product content about how to address them. Follow the documented guidelines to resolve the issues in each of the findings.

### Monitor user, email, and antivirus metrics

Monitor user, email, or antivirus metrics for your instance. For example, you can monitor your email security by checking metrics for spam, external emails, and inbound emails from untrusted and trusted domains for your instance. Analyze these metrics to look for anomalous security behaviors that are related to activities that take place in your instance.

### User metrics

Analyze user metrics to look for anomalous behaviors that are related to specific types of user activity in your instance.

#### Not Logged in Last Month / Last Six Months / Last Year

Indicates the number of users who have not logged into the instance within the last month, within the last six months, and within the last calendar year. To view user detail for a specific metric:

- Click the metric to view a listing of users that have not logged in to the instance during the indicated time period.
- Click a user name to view more details about that user.

#### Users with High Privilege Roles

Indicates the number of users with the following high privilege role types:

<table>
<thead>
<tr>
<th>User role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>Primary administrator role that has access to all system features, functions, and data, regardless of security constraints.</td>
</tr>
<tr>
<td>script_include_admin</td>
<td>Administrator role that also has access to script includes.</td>
</tr>
<tr>
<td>password_reset_admin</td>
<td>Administrator role that enables a user to view the status of password reset activities, identify potential security threats, and monitor for compliance with password security policies. To learn more, see Password Reset and Password Change reports and logs.</td>
</tr>
<tr>
<td>User role</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>security_admin</td>
<td>Elevated privilege role that enables a user to create and change access controls and High Security Settings. To learn more, see security_admin role</td>
</tr>
<tr>
<td>user_admin</td>
<td>Administrator role that can also manage users, roles, user groups, roles, and department assignments.</td>
</tr>
</tbody>
</table>

**Note:** To learn more about these administrative role types, see Special administrative roles.

To view user detail for a specific user role metric:
- Click the user count role metric to view a listing of users with that high privilege role type.
- Click a user name to view more details about that user. You can then determine if these security-critical roles are assigned to the proper personnel.

**Users Trend**

Shows count trend information over a time period for the following types of users:

<table>
<thead>
<tr>
<th>Count type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Users</td>
<td>Number of users who are marked as Active in the instance.</td>
</tr>
<tr>
<td>Inactive Users</td>
<td>Number of users who are marked as Inactive in the instance.</td>
</tr>
<tr>
<td>Locked Out</td>
<td>Number of users who are locked out of the instance.</td>
</tr>
</tbody>
</table>

To view user detail for a specific user count (for example, Locked Out Users):
- Click the Locked out users metric.
- In the Analytics Hub page, click Show Records.
- Click a user name to view more details about that user. You can then determine if there is a reason this person is locked out and remedy the situation.

**Events Trend**

Shows count trend information for specific types of events, over a time period:

<table>
<thead>
<tr>
<th>Event type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin login</td>
<td>Number of users with high privilege administrator user roles who logged in on a specific day.</td>
</tr>
<tr>
<td>External login</td>
<td>Number of users with an assigned snc_external role who logged into this instance during the calendar day. These logins typically occur for maintenance, support, consulting, or audit purposes. Monitoring this metric enables you to verify that the external login attempts are legitimate and not potential security issues.</td>
</tr>
<tr>
<td>Failed login</td>
<td>Number of failed login attempts on a specific day.</td>
</tr>
<tr>
<td>Impersonation</td>
<td>Number of users logged in on a specific day who are impersonating other users.</td>
</tr>
<tr>
<td>Event type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Security elevation</td>
<td>Number of times that a security administrator has elevated security for standard users by changing their assigned user role to a high privilege security role during the calendar day. These high privilege security roles include oauth_admin, admin, security_admin, and impersonator.</td>
</tr>
<tr>
<td>SNC login</td>
<td>Number of Customer Service and Support who logged in to this instance using the hopping technique during a specific day.</td>
</tr>
</tbody>
</table>

To view user detail for a specific event count (for example, Impersonation):

- Click the user count metric. The Security Dashboard Event Logs page lists event logs for that type of event.
- Click a user name to view more details about that event.

### Email metrics

Analyze your email metrics to look for anomalous behaviors that are related to the incoming emails to your instance. For example, if the metrics indicate a spike in spam emails from specific domains, you can define inbound actions that prevent their delivery to the instance.

For each email metric, a count appears for each type of email that is delivered or sent to the instance during the calendar day.

<table>
<thead>
<tr>
<th>Notification preference</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Incoming Email</td>
<td>Number of incoming emails for the calendar day that were delivered to the instance from external email domains.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The external email domains are those domains that are not listed in the security.list.internal.domains system property, because this property tracks only your internal email domains. To learn more about this property, see Available system properties.</td>
</tr>
<tr>
<td>Spam</td>
<td>Number of incoming emails for the calendar day that were delivered to the instance and marked as spam. A number that is out of line with historical trends may indicate that attempts are being made to compromise your instance security.</td>
</tr>
<tr>
<td>Trusted Incoming Email</td>
<td>Number of incoming emails to the instance for the calendar day from email domains designated as trusted.</td>
</tr>
<tr>
<td>Untrusted Incoming Email</td>
<td>Number of incoming emails to the instance for the calendar day from email domains designated as untrusted.</td>
</tr>
<tr>
<td></td>
<td>You can designate untrusted or trusted email domains in the Untrusted And Trusted Domain form so that you can track your inbound emails that are sent from them. To learn how to designate untrusted or trusted email domains, see Designate email domains as untrusted or trusted.</td>
</tr>
</tbody>
</table>

After you click an email metric, you can learn about the possible email security issues in your instance by clicking one of the following:
### Command | Description
--- | ---
Chart | Incoming email counts and count trends over time for the selected email type (spam, incoming external, untrusted, or trusted).
Records | Individual email records that compromise the daily count for the selected email type.
More Info | Additional information for the selected email type.

**Note:** The email metrics apply only to your incoming emails to the instance. The metrics do not apply to the normal traffic that is processed through your enterprise-wide email servers. To learn about defining inbound actions and how they impact the processing of your inbound emails, see Inbound email actions.

#### Designate email domains as untrusted or trusted
Designate specific email domains as untrusted or trusted so that you can monitor the metrics for incoming emails from these sources in your instance.

Role required: security_dashboard_user or admin

When untrusted or trusted domains send emails to your instance, their daily counts appear on the **Untrusted Incoming Email** or **Trusted Incoming Email** metrics on the Email page. You can then track email activity from these domains and use email logs to view specific incoming emails. You can also specify a user, usually a manager, or a security analyst, to notify whenever activity occurs from the untrusted or trusted domain.

**Note:** Designating an email domain as untrusted is for security tracking purposes only. Administrators can also set up a system address filter to ignore emails from untrusted domains. To learn about filtering emails to block their delivery, see System address filters.

1. Navigate to **System Security > Instance Security Center**.
2. On the Instance Security Center homepage, click the **Email** tile, or click the **Email** link to access the Email page.
3. On the Email page, in the Untrusted And Trusted Domain section, click **New**.
4. On the form, fill in the fields.

#### Untrusted And Trusted Domain form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Name of the email domain that you are designating as untrusted or trusted. For example, enter servicenow.com to designate ServiceNow employees can send trusted emails to the instance.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Category</td>
<td>Category that indicates if the email domain is untrusted or trusted:</td>
</tr>
<tr>
<td></td>
<td><strong>Untrusted</strong></td>
</tr>
<tr>
<td></td>
<td>Designates that the email domain as untrusted. You use it to identify domains that send suspicious or emails that pose a potential security threat to the instance.</td>
</tr>
<tr>
<td></td>
<td><strong>Trusted</strong></td>
</tr>
<tr>
<td></td>
<td>Designates that the email domain as trusted. You use it to identify domains when your metrics indicate that the incoming emails from it pose no security threats. Designating the domain as trusted enables you to track its inbound email activity over time.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box for enabling or disabling the designated untrusted or trusted status for the specified email domain.</td>
</tr>
<tr>
<td>Notify</td>
<td>Name of the user to notify by email when activity occurs in the untrusted or trusted domain. Click the spotlight search icon (</td>
</tr>
<tr>
<td></td>
<td>) to search for the name of the user. Leave the Notify field blank if you do not want notifications sent.</td>
</tr>
</tbody>
</table>

5. Click **Save**.

Untrusted or trusted email domain information is also added to the **Untrusted And Trusted Domains** listing on the Email page.

**Antivirus metrics**

If the Antivirus Scanning plugin is activated, Antivirus Scanning runs in your instance to help protect it against virus infections from attachments.

The following metrics appear for the last 60 days of activity, and enable you to assess the effectiveness of the Antivirus Scanning functions.

**Antivirus Events**

Antivirus Events indicate the number of antivirus events in your instance, by date. To access the antivirus events, navigate to **System Security > Instance Security Center** and select the Metrics tab. Color coded graph lines represent the following types of antivirus events:

<table>
<thead>
<tr>
<th>Color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blue</td>
<td>Number of files quarantined by Antivirus Scanning in this instance for the indicated date.</td>
</tr>
<tr>
<td>Green</td>
<td>Number of infected files downloaded to the instance, and then quarantined for the indicated date. These files are primarily email attachments that contain a virus or rouge code.</td>
</tr>
<tr>
<td>Color</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Yellow</td>
<td>Number of quarantined files in the instance that were deleted for the indicated date.</td>
</tr>
<tr>
<td>Orange</td>
<td>Number of quarantined files in the instance that were restored for the indicated date.</td>
</tr>
</tbody>
</table>

**Note:** After Antivirus Scanning runs and finds any false positives, you can restore a quarantined file and make it accessible in the instance.

- To access the Analytics Hub page and view the detailed score card and analytics information for a specific date, click a colored line in the Antivirus Events graph. For example, click the blue graphics line to view analytics information for files quarantined for a specific date.
- To view the following breakdowns in the Analytics Hub page, click

  ![icon]

  then click:

<table>
<thead>
<tr>
<th>Breakdown</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AppSec - Antivirus Event Source</td>
<td>Source of the antivirus event.</td>
</tr>
<tr>
<td>• On Upload: Occurred due to an upload of an infected file, usually an attachment.</td>
<td></td>
</tr>
<tr>
<td>• From Quarantine: Occurred due to the quarantine of an infected file, usually an attachment.</td>
<td></td>
</tr>
<tr>
<td>• On Download: Occurred due to a download of an infected file, usually an attachment.</td>
<td></td>
</tr>
<tr>
<td>• From Record: Occurred due to an infected record in a table.</td>
<td></td>
</tr>
<tr>
<td>AppSec - Antivirus Event Type</td>
<td>Type of antivirus event.</td>
</tr>
<tr>
<td>• Quarantined: Occurred due to the quarantine of a file, usually an attachment.</td>
<td></td>
</tr>
<tr>
<td>• Downloaded: Occurred due to a download of a file, usually an attachment.</td>
<td></td>
</tr>
<tr>
<td>• Restored: Occurred due to the restoration of a quarantined file.</td>
<td></td>
</tr>
<tr>
<td>• Deleted: Occurred due to the deletion of a quarantined file.</td>
<td></td>
</tr>
<tr>
<td>AppSec - Antivirus Uploader</td>
<td>Name of the logged in user who uploaded the files that were the source of virus infections detected by the Antivirus Scanning application.</td>
</tr>
</tbody>
</table>

### Quarantined Files

Lists the infected files in the instance quarantined by Antivirus Scanning:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File name</td>
<td>Name of the infected file.</td>
</tr>
<tr>
<td>Content type</td>
<td>Type of content that was infected in the file. For example, application/x-dosexec is an infected application or DOS executable file, while text/plain is an infected .txt file.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
**Table** | Name of the table that contains the infected file. For example, *incident* appears for an incident file record.

**Virus** | Name of the file quarantined by Antivirus Scanning.

**Detected** | Date and time the infected file was detected.

**Created By** | Name of the user who quarantined the infected file.

**Created** | Date and time the quarantine file record was created.

**Table sys ID** | Table system identifier assigned to the quarantine file record.

---

**Note:** You can also add Quaranatined Files and Virus Types tiles to the Event ribbon. To learn more, see Monitor security events and Configure the security event ribbon.

### Activate the ISC Virtual Agent interface

If you have the admin role, you can activate the ISC Virtual Agent Conversations plugin (com.glide.isc_virtualagent). Activating this plugin installs the Virtual Agent and Natural Language Understanding (NLU) content packs, providing Virtual Agent access from the Instance Security Center.

The Virtual Agent interface in the Instance Security Center is only available for users with paid Virtual Agent subscriptions, and who have activated the Glide Virtual Agent (com.glide.cs.chatbot) plugin. To learn more, see Activate Virtual Agent.

Role required: admin

To learn more about the accessing the Virtual Agent from the Instance Security Center, see Virtual Agent access in the Instance Security Center.

#### Plugins for ISC Virtual Agent

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISC Virtual Agent Conversations [com.glide.isc_virtualagent]</td>
<td>Activates the ISC Virtual Agent Conversations content pack for the Instance Security Center.</td>
</tr>
</tbody>
</table>


**Note:** Activating the com.glide.isc_virtualagent plugin automatically activates com.glide.isc_nlu. However, if you activate the com.glide.isc_nlu plugin first, you must manually activate com.glide.isc_virtualagent as well.

1. Navigate to **System Applications > All Available Applications > All.**
2. Find the plugin using the filter criteria and search bar.

You can search for the plugin by its name or ID. If you cannot find a plugin, you might have to request it from ServiceNow personnel. For more information, see Request a plugin.
3. Click **Install**, and then in the Activate Plugin dialog box, click **Activate**.

**Note:** When domain separation and delegated admin are enabled in an instance, the administrative user must be in the **global** domain. Otherwise, the following error appears: Application installation is unavailable because another operation is running: Plugin Activation for **<plugin name>**.

---

**General security settings properties**

Security settings provide several properties to control the level of security on your instance. There are several ways to set or change general security settings properties.

- **Navigate to** **System Properties > Security**.
  
  Options on the Security page are **Yes** or **No**.

- **Navigate to the** **sys_properties.list** and search for the property you want to set or change.
  
  Options in the System Properties table [sys_properties.list] are **true** or **false**.

- **Navigate to** **System Security > Instance Security Center**, then click **Hardening**.
  
  You can configure the settings for the most important and critical security properties. The Instance Security Hardening Settings content contains detailed descriptions, and compliance values, for the security-related system properties and plugins in the **. To learn more about each of these properties, see Instance Security Hardening Settings.**

**Warning:** When implementing any of these security features, you must thoroughly test the features before you deploy them in a production instance.

---

**Escaping and embedded script support**

**glide.ui.security.allow_codetag**

Supports embedding HTML code using the [code] tag.

- Default value: Yes
- Instance Security Hardening Settings: Allow embedded HTML code (instance security hardening)

**glide.ui.security.codetag.allow_script**

Allows embedded HTML (using [code] tags) to contain Javascript tags.

- Instance Security Hardening Settings: Allow JavaScript tags in embedded HTML (instance security hardening)

**glide.ui.escape_all_script**

Forces all expressions within Jelly JavaScript `<script type="text/javascript">` tags to be escaped by default. Enforces escaping only if the type attribute in the `<script>` tag is empty, or if the value is `text/javascript`, `text/ecmascript`, `application/javascript`, `application/ecmascript`, or `application/x-javascript`.

- Default value:
  - New/zbooted instances: Yes
  - Upgraded instances: No
• Recommended value: Yes
• Instance Security Hardening Settings: Escape Jelly (instance security hardening)

Attachment limits and behavior

**com.glide.attachment.max_size**
Sets the maximum file attachment size in megabytes.

**glide.attachment.role**
Lists the roles (comma-separated) that can create attachments.

**glide.attachment.extensions**
Lists the file extensions (comma-separated) that can be attached to documents via the attachment dialog. Extensions should not include the dot (.). For example, xls, xlsx, doc, docx. Leave blank to allow all extensions.
• Instance Security Hardening Settings: Restrict file extensions (instance security hardening)

**glide.ui.attachment.force_download_all_mime_types**
Forces download of all multipurpose internet mail extensions (MIME) type attachment files.
• Default value:
  • New/zbooted instances: Yes
  • Upgraded instances: No
  • Instance Security Hardening Settings: Force Download MIME types (instance security hardening)

**glide.security.file.mime_type.validation**
Enables (Yes) or disables (No) MIME type validation for file attachments. File extensions configured via **glide.attachment.extensions** are checked for MIME type during upload.
• Default value:
  • New/zbooted instances: Yes
  • Upgraded instances: No
  • Instance Security Hardening Settings: Upload MIME type restriction (instance security hardening)

Customer uploads

These properties affect customer uploads only. They do not affect attachments.

**glide.ui.strict_customer_uploaded_static_content**
When you set this property to Yes, turns on the ability to restrict the types of files that can be downloaded, when they have been uploaded using the Upload File functionality of the Now Platform. Used with **glide.ui.strict_customer_uploaded_content_types**
• Instance Security Hardening Settings: Enable file download restrictions (instance security hardening)

**glide.ui.strict_customer_uploaded_content_types**
When this parameter includes a list of comma-delimited file types, of the files that were uploaded using the Upload File functionality of the Now Platform, only these file types can be downloaded from the instance.

- **Instance Security Hardening Settings:** Downloadable file types (instance security hardening)

**Security Manager and options**

**glide.security.manager**
Security Manager.

**glide.sm.default_mode**
Security manager default behavior in the absence of any ACLs on a table.

**glide.security.strict.updates**
Double-checks security on inbound transactions during form submission. Rights are always checked on form generation.

- **Instance Security Hardening Settings:** Double check inbound transactions (instance security hardening)

**glide.security.strict.actions**
Checks conditions on UI actions before execution. Normally, conditions are checked only during form rendering.

- **Instance Security Hardening Settings:** Check UI action conditions before execution (instance security hardening)

**glide.security.granular.create**
Enforces the create rules on new records (as opposed to the write rules, which may include creating and updating).

**glide.security.explain.write.locks**
Displays an explanation on locked form elements.

**Cookies**

**glide.ui.forgetme**
Removes the Remember me check box from the login page when the instance is using either LDAP or DB logins. User’s active logged in sessions are timed out after X minutes of inactivity, where X is the value of the glide.ui.session_timeout system property.

- Default value:
  - New/zbooted instances: Yes

- **Instance Security Hardening Settings:** Remove remember me (instance security hardening)

**glide.ui.secure_cookies**
Enables secure session cookies to enforce additional cookie security. If Yes, strict session cookie validation is enforced. With version 3 cookies enabled, additional security requirements are also enforced.

- **Instance Security Hardening Settings:** Secure session cookies (instance security hardening)

**glide.secure_cookie.debug**
Secure session cookie debugging. Select to enable extensive debug logging of secure session cookie operations.

**Security restrictions for execution of scripts originating from the client**

**glide.script.use.sandbox**
Run client-generated scripts (AJAXEvaluate and query conditions) inside a reduced-rights sandbox. If enabled, only those business rules and script includes with the Client callable check box selected are available, and certain back-end application programming interface (API) calls are disallowed.

- Instance Security Hardening Settings: Client generated scripts sandbox (instance security hardening)

**glide.script.allow.ajaxevaluate**
Enables the AJAXEvaluate processor.

- Instance Security Hardening Settings: Enable AJAXEvaluate (instance security hardening)

**glide.script.secure.ajaxgliderecord**
Applies standard security access control lists (ACLs) to AJAXGlideRecord calls.

- Default value: Yes for new and upgraded instances. If Yes, cannot be changed to No.
- Instance Security Hardening Settings: Enabling AJAXGlideRecord ACL checking (instance security hardening)

**Miscellaneous**

**com.glide.communications.trustmanager_trust_all**
By default, the instance trusts a certificate's Certificate Authority (CA). Ensures that the instance accepts self-issued certificates. To validate a certificate's CA, set this property to No.

- Instance Security Hardening Settings: Certificate trust (instance security hardening)

**glide.outbound.sslv3.disabled**
When active, forces outbound connections from an instance to use the transport layer security (TLS) instead of the secure sockets layer (SSL).

- Instance Security Hardening Settings: Disabling SSLv2/SSLv3 (instance security hardening)

Additional properties are available for High Security Settings.

**High Security Settings**

High Security Settings refer to several security options available in your instance.

The High Security Settings module is activated with the High Security Settings plugin, which is active by default on new instances. If High Security Settings are not active on your instance, see Requesting High Security Settings activation. To learn more about this plugin, see High security plugin (instance security hardening) in Instance Security Hardening Settings. Properties for these types of high security settings are available:

- Default property values: To harden security on your platform by centralizing all critical security settings to one location for management and auditing.
• Default deny property: Provides a security manager property to control the default security behavior for table access.
• Security Administrator role: Provides a role to prevent modification of key security settings and resources. The Security Administrator role is not inherited by the admin role and must be explicitly assigned.
• Elevated privileges: Allows users with the security admin role to operate in the context of a normal user and elevate to higher security role when needed.
• Property access controls: Allows security administrators to set the roles required to read and write properties.
• Transaction and system logs: Are read only.
• Access control rules: Control what data users can access and how they can access it.

Note: High Security Settings also automatically activates the Contextual Security plugin, if it is not already active. In addition, Platform Security Settings - High delivers settings and features in the context of increasing the security of your instance.

Note:

Note: The Instance Security Hardening Settings content contains detailed descriptions, and compliance values, for the security-related system properties and plugins in the . To learn more about each of these properties, see Instance Security Hardening Settings.

There are two ways to set or change High Security Settings properties.

• Navigate to System Security > High Security Settings.
  Options on the High Security Properties page are Yes or No.
• Navigate to the sys_properties.list and search for the property you want to set or change.
  Options in the System Properties table [sys_properties.list] are true or false.

Property access control

Two additional columns are created in the Properties [sys_properties] table when High Security Settings are active:

• read_roles: A comma-separated list of role names that are allowed to read all fields of this property.
• write_roles: A comma-separated list of role names that are allowed to write/modify all fields of this property.

Properties listed in the Properties table have read_roles of admin, and write_roles of security_admin. Users with the admin role can view and read the property values, but must elevate to the security_admin role to modify them.

Notifications

Activation of high security settings also activates security warning messages. The following is an example of a message that appears after an approval.
Security Warning notification

High Security Settings properties

**glide.ui.escape_text**

Escape XML values at the parser level for the user interface. Prevents reflected and stored cross-site scripting attacks. This property is not applicable in Service Portal.

- Default value: Yes
- Instance Security Hardening Settings: Escape XML (instance security hardening)

**glide.ui.escape_all_script**

Forces all expressions within Jelly JavaScript `<script type="text/javascript">` tags to be escaped by default. Enforces escaping only if the type attribute in the `<script>` tag is empty, or if the value is `text/javascript`, `text/ecmascript`, `application/javascript`, or `application/x-javascript`.

- Default value: Yes in new instances
- Instance Security Hardening Settings: Escape Jelly (instance security hardening)

**glide.ui.rotate_sessions**


- Default value: Yes
  - If you are using the SAML 2.0 plugin for Single Sign-on authentication, set this property to No. Otherwise, it interferes with the session information sharing that takes place between the instance and the Identity Provider.
- Instance Security Hardening Settings: Rotate HTTP session identifiers (instance security hardening)

**glide.ui.secure_cookies**

Enable secure session cookies: Enable additional cookie security. If **Yes**, strict session cookie validation is enforced.

- Default value: Yes
• Instance Security Hardening Settings: Secure session cookies (instance security hardening)

**glide.security.password_reset.uri**

For mobile Password Reset, URL that the user is taken to when the user clicks the **Forgot password?** button.

**glide.security.strict.updates**

Double-check security on inbound transactions during form submission (rights are always checked on form generation).

- Default value: Yes
- Instance Security Hardening Settings: Double check inbound transactions (instance security hardening)

**glide.security.strict.actions**

Check conditions on UI actions before execution. Normally conditions are checked only during form rendering.

- Default value: Yes
- Instance Security Hardening Settings: Check UI action conditions before execution (instance security hardening)

**glide.security.use_csrf_token**

Enable usage of a secure token to identify and validate incoming requests. This token is used to prevent cross-site request forgery attacks.

- Default value: Yes
- Instance Security Hardening Settings: Anti-CSRF token (instance security hardening)

**glide.ui.escape_html_list_field**

Escape HTML for HTML fields in a list view.

- Default value: Yes
- Instance Security Hardening Settings: Escape HTML (instance security hardening)

**glide.html.escape_script**

Escape JavaScript tags in HTML fields.

- Default value: Yes
- Instance Security Hardening Settings: Escape JavaScript (instance security hardening)

**glide.ui.forgetme**

Remove the **Remember me** check box from the login page.

- Default value: Yes
- Instance Security Hardening Settings: Remove remember me (instance security hardening)

**glide.smtp.auth**

Authenticate with the SMTP server by the user name and password properties.

- Default value: Yes
- Instance Security Hardening Settings: SMTP authentication (deprecated)

**Note:** This property is deprecated.
glide.script.use.sandbox
Run client-generated scripts (AJAXEvaluate and query conditions) inside a reduced-rights sandbox. If Yes, only those business rules and script includes with the Client callable check box set to Yes are available, and certain back-end API calls are disallowed. For more information, see Script sandbox property.

- Default value: Yes
- Instance Security Hardening Settings: Client generated scripts sandbox (instance security hardening)

glide.soap.strict_security
Enforce strict security on incoming SOAP requests. Requires incoming SOAP requests to go through the security manager for table and field access and checks SOAP users for the correct roles for using the web service.

- Default value: Yes
- Instance Security Hardening Settings: SOAP request strict security (instance security hardening)

Note: If you choose not to require authorization for incoming WSDL requests, you must modify the Access Control (ACL) rules to allow guest users to access the WSDL content.

glide.basicauth.required.wsd
Require authorization for incoming WSDL requests.

- Default value: Yes
- Instance Security Hardening Settings: WSDL request authorization (instance security hardening)

Note: If you choose not to require authorization for incoming WSDL requests, you must modify the Access Control (ACL) rules to allow guest users to access the WSDL content.

glide.basicauth.required.csv
Require basic authorization for incoming CSV requests.

- Default value: Yes
- Instance Security Hardening Settings: CSV request authorization (instance security hardening)

glide.basicauth.required.excel
Require basic authorization for incoming Excel requests.

- Default value: Yes
- Instance Security Hardening Settings: Excel request authorization (instance security hardening)

glide.basicauth.required.importprocessor
Require basic authorization for incoming import requests.

- Default value: Yes
- Instance Security Hardening Settings: Import request authorization (instance security hardening)

glide.basicauth.required.pdf
Require basic authorization for incoming PDF requests.

- Default value: Yes
- Instance Security Hardening Settings: PDF request authorization (instance security hardening)

glide.basicauth.required.rss
Require basic authorization for incoming RSS requests.
• Default value: Yes
• Instance Security Hardening Settings: RSS request authorization (instance security hardening)

**glide.basicauth.required.scriptedprocessor**

Require basic authorization for incoming script requests.

• Default value: Yes
• Instance Security Hardening Settings: Script request authorization (instance security hardening)

**glide.basicauth.required.soap**

Require basic authorization for incoming SOAP requests.

• Default value: Yes
• Instance Security Hardening Settings: Basic auth: SOAP requests (instance security hardening)

**glide.basicauth.required.unl**

Require basic authorization for incoming unload requests.

• Default value: Yes
• Instance Security Hardening Settings: Unload request authorization (instance security hardening)

**glide.basicauth.required.xml**

Require basic authorization for incoming XML requests.

• Default value: Yes
• Instance Security Hardening Settings: XML request authorization (instance security hardening)

**glide.basicauth.required.xsd**

Require basic authorization for incoming XSD requests.

• Default value: Yes
• Instance Security Hardening Settings: XSD request authorization (instance security hardening)

**glide.cms.catalog_uri_relative**

Enforce relative links from the URI parameter on /ess/catalog.do. If **Yes**, only relative URLs are permitted through the /ess/catalog.do page using the **uri** parameter. If **No**, all URLs are permitted, which may permit linking to external unauthorized content.

• Default value: Yes
• Instance Security Hardening Settings: Enforce relative links (instance security hardening)

**glide.set_x_frame_options**

Enable this property to set the X-Frame-Options response header to SAMEORIGIN for all UI pages. The X-Frame-Options HTTP response header can be used to indicate whether a browser should be allowed to render a page in a <frame> or <iframe>. Sites can use this property to avoid clickjacking attacks by ensuring that their content is not embedded into other sites. [https://developer.mozilla.org/en/the_x-frame-options_response_header](https://developer.mozilla.org/en/the_x-frame-options_response_header)

• Default value: Yes
• Instance Security Hardening Settings: X-Frame-Options: SAMEORIGIN (instance security hardening)

**glide.ui.attachment.download_mime_types**
A list of comma-separated attachment mime types that do not render inline in the browser. Prevents cross-site scripting attacks. For example, `text/html` forces HTML files to be downloaded to the client as attachments rather than viewed inline in the browser.

- Default value: `text/html, image/svg, image/svg+xml`
- Instance Security Hardening Settings: Force Download MIME types (instance security hardening)

**glide.security.groupby_acl_check**

When this property is enabled, ACL checks for GroupBy operations are performed for the group names based on the actual data from the groups.

- Default value: Yes

**glide.security.diag_txns_acl**

If Yes, only the admin user or user from allowed IP address can access `stats.do`, `threads.do`, and `replication.do`.

- Default value: No
- Instance Security Hardening Settings: Performance monitoring (ACL) (instance security hardening)

**glide.ui.security.codetag.allow_script**

Allow embedded HTML (using `[code]` tags) to contain JavaScript tags.

- Default value: Yes
- Instance Security Hardening Settings: Allow embedded HTML code (instance security hardening)

**glide.script.allow.ajaxevaluate**

Enable the AJAXEvaluate processor. The AJAXEvaluate API call allows the client to send and execute arbitrary scripts on the server.

- Default value: No
- Instance Security Hardening Settings: Enable AJAXEvaluate (instance security hardening)

**glide.login.autocomplete**

Allow browsers to use auto-complete on password fields on login forms.

- Default value: No
- Instance Security Hardening Settings: Password field auto-complete (instance security hardening)

The following properties are defined in the `sys_properties` table, but are not visible on the High Security Settings page.

**com.glide.communications.httpclient.verify_hostname**

Verify the hostname and certificate chain presented by remote SSL hosts. Protect against Man-In-The-Middle (MITM) attacks.

- Default value: true
- Learn more: Set up Kubernetes spoke

**Note:** This property overrides the `com.glide.communications.trustmanager_trust_all` property.

**glide.basicauth.required.schema**
Require basic authentication for inbound table schema requests.

- Default value: true

**glide.security.csrf_previous.allow**
Allow usage of an expired secure token to identify and validate incoming requests. This token is used to prevent cross-site request forgery attacks.

- Default value: false

**glide.security.csrf_previous.time_limit**
Time in seconds for a secure token to expire. Allows control over the length of time that the previous CSRF token is valid. When the user session expires, the secure token expires with it unless the **glide.security.csrf_previous.allow** property is enabled and it is within the timeframe described by this property. This token is used to prevent cross-site request forgery attacks.

- Default value: 86400 seconds or 1 day

**glide.security.csrf.strict.validation.mode**
Enforces strict validation on CSRF tokens so that users cannot resubmit a request if the CSRF token does not match.

- Default value: false
- Instance Security Hardening Settings: CSRF strict validation (instance security hardening)

**com.glide.security.check.unsanitized.html**
Enforces sanitization behavior of translated_html fields on a global level for field assignments.

- Default value: enforce

### Script sandbox property
Enable the script sandbox property (**glide.script.use.sandbox**) to run client generated scripts inside a sandbox that has restricted rights.

There are two cases within the system that allow the client to send scripts to the server for evaluation.

- Filters and/or queries: It is legal to send a filter to the server such as:
  
  `assigned_to=javascript:getMyGroups()`.

- System API: The API call `AJAXEvaluate` allows the client to run arbitrary scripts on the server and receive a response.

If you enable the script sandbox property (**glide.script.use.sandbox**), the script being evaluated via either of these two entry points runs within a reduced rights sandbox with the following characteristics:

- Only those business rules marked **client callable** are available within the sandbox.
- Only script includes marked **client callable** are available within the sandbox.
- Certain API calls (largely but not entirely limited to those dealing with direct DB access) are not allowed.
- Data cannot be inserted, updated, or deleted from within the sandbox. Any calls to `current.update()` for example, are ignored.

**Note:** To learn more about this property, see Client generated scripts sandbox (instance security hardening) in Instance Security Hardening Settings.
These methods are not allowed in client scripts when script sandboxing is enabled.

### Restricted methods

<table>
<thead>
<tr>
<th>Class</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>GlideRecord</td>
<td>deleteMultiple(), deleteRecord(), insert(), update(), updateMultiple()</td>
</tr>
<tr>
<td>GlideSystem (gs)</td>
<td>addErrorMessage(), addInfoMessage(), addMessage(), eventQueue(),</td>
</tr>
<tr>
<td></td>
<td>flushMessages(), getEscapedProperty(), getProperty(), setProperty(),</td>
</tr>
<tr>
<td></td>
<td>setRedirect(), setReturn(), workflowFlush()</td>
</tr>
<tr>
<td>ScopedGlideRecord</td>
<td>deleteMultiple(), deleteRecord(), insert(), update(), updateMultiple()</td>
</tr>
<tr>
<td>ScopedGlideSystem (gs)</td>
<td>addErrorMessage(), addInfoMessage(), eventQueue(), executeNow(),</td>
</tr>
<tr>
<td></td>
<td>getProperty(), getSessionToken(), setRedirect()</td>
</tr>
</tbody>
</table>

If you run the system without script sandboxing enabled, then none of these restrictions apply.

**Note:** This property is activated by default when you activate the High Security Settings plugin. Do not activate this property outside of the plugin.

<table>
<thead>
<tr>
<th>Property</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run client generated scripts (AJAXEvaluate and query conditions) inside a reduced rights &quot;sandbox.&quot;</td>
<td>Enabled (sandbox in use)</td>
</tr>
<tr>
<td>If enabled, only those business rules and script includes with the <strong>Client callable</strong> checkbox set to true are available and certain back-end API calls are disallowed.</td>
<td></td>
</tr>
</tbody>
</table>

### Request High Security Settings activation

The High Security Settings plugin is active by default on all new instances. If it is not active on your instance, you can request the plugin.

Before activating High Security Settings on an existing instance:

1. Review the following information to understand the new behavior:
   - Access control list rules
   - High Security Settings
   - Default deny property
2. Enable the plugin on a non-production instance. A recent clone of production is preferable.
3. Test the revised functionality, especially the added ACLs and default-deny functionality. Continue testing until the system performs as expected. If users cannot access expected resources, ensure they have appropriate roles and ACL rules to grant them the access.
4. Create update sets of any needed changes so you can apply them to production.
Role required: admin

1. Navigate to **System Applications > All Available Applications > All.**
2. On the All Applications page, click **Request Plugin** to open the Request form on HI.
3. On Now Support, select the redirect link to access the Now Support Service Portal Service Catalog.

<table>
<thead>
<tr>
<th>Activate Plugin</th>
</tr>
</thead>
<tbody>
<tr>
<td>In order to enhance the user experience, we have redesigned Activate a Plugin service catalog. Please use the new HI Service Portal ‘Activate a Plugin’ service catalog item. You can also use Manage Instances page on Service Portal to Activate a Plugin.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Instance</td>
<td>Instance on which to activate the plugin.</td>
</tr>
<tr>
<td>Plugin Name</td>
<td>Name of the plugin to activate.</td>
</tr>
<tr>
<td>Specify the date and time you would like this plugin to be enabled</td>
<td>The date and time must be at least two business days from the current time.</td>
</tr>
</tbody>
</table>

**Note:** Plugins are activated in two batches, once in the morning and once in the evening, on every business day in the US Pacific time zone. If the plugin must be activated at a specific time, enter the request in the **Reason/Comments** field.

| Reason/Comments | Information that would be helpful for the ServiceNow personnel who are activating the plugin. For example, if you need the plugin activated at a specific time instead of during one of the default activation windows, specify that in the comments. |

5. Click Submit.

**ServiceNow access control**

This SNC Access Control plugin (com.snc.snc_access_control) enables you to control which Customer Service and Support employees can access your instance, and when.

When you first activate the plugin, Customer Service and Support employees cannot log into the instance. Any currently logged-in Customer Service and Support employees remain logged in. You create records in the SNC Access Control table that grant access to specific SNC employees or all employees.

The plugin prevents Customer Service and Support personnel from accessing the instances without your express permission. However, other authorized ServiceNow Operations personnel, in their capacity to support and manage the product, are required to perform administrative actions on the underlying infrastructure. This infrastructure includes servers and databases, among other infrastructure components that make up the SaaS solution. This access method is fully auditable and tracked.
This plugin enables you to restrict access to your instance without your express permission, so it may affect support service levels and the Availability SLA. Availability SLA is then measured from the time that Support staff personnel are granted access to your instance.

**Login security**

Security for authorized Customer Service and Support employee logins to instances employs encrypted tokens generated by a secure server. Only properly authenticated Customer Service and Support employees are granted access to an instance. Without the SNC Access Control plugin, the security server ensures that access rights are enforced on hi.service-now.com. When the plugin is enabled, the encrypted login tokens must match names in the plugin-provided access list, using the criteria defined in those records. This method of authentication enables you to determine precisely which Customer Service and Support employees may access their instances, and when these employees may do so.

The architecture chosen for this system has several features designed to enhance security for your instances:

**Security server**

The security server is a locked-down, Linux host that only ServiceNow security personnel can access. This server is the only system that has access to the critical private encryption key necessary to produce the login tokens. By using this compartmentalization (a standard security practice), the private key is protected, even in the unlikely event that an attacker compromises the HI instance.

**Synthetic user**

The facility on instances that enables authorized Customer Service and Support employees to log into their instance does not require an account to be provisioned on that instance. There is no user record provisioned, and no permanent or persisted credentials. Instead, a synthetic user is created for each Customer Service and Support employee logon. This user exists only in memory and provides no ongoing privileges. If the SNC Access Control plugin is enabled, you can deauthorize any Customer Service and Support employee at any time.

**Tokens**

The security tokens are specific to an instance and a particular Customer Service and Support employee. In addition, the mechanism that generates the tokens only works with actual Customer Service and Support employee logins to HI, not impersonated users. Once a security token is generated, only a specific Customer Service and Support employee can use it to log into an instance.

**Time limit**

Security tokens expire four hours after they are generated. This expiration limits the utility of hijacked tokens, which can only be used during this short window.

**Logging**

Logins by Customer Service and Support employees to instances are recorded as a login event.

- Every action taken by the logged-in Customer Service and Support employee is added to the transaction log in the database.
- It is also added to the instance log on the file system, which is inaccessible to most ServiceNow employees.
- Customer Service and Support employee logins and actions are readily identifiable, since the user names all end in @snc (like frodo.baggins@snc).

These actions provide you with easy-to-use, robust, and reliable security logging for non-employee access.
Security processing flow

When a Customer Service and Support employee wants to log into an instance, the security processing flow is as follows:

2. HI checks that the technician has the proper role authorizing access to instances.
3. If the user has the proper role, HI sends the request for access to the Security Server.
4. The Security Server verifies that the request came from the HI IP address, and evaluates the request (user, role, and IP address of the requester). If the request is valid, the Security Server approves it and constructs a token. This token contains the user name, roles, the instance ID, and the time (the start of the 4-hour token life span). Finally, the Security Server encrypts the token with the private encryption key.
5. The Security Server sends the encrypted token to HI.
6. Hi sends the token to the Support technician's browser.
7. The Support technician's browser initiates a login into the instance, using the special user name ending with @snc.
8. The instance uses the public key to decrypt the token. To verify the token, the instance matches it to the user name supplied in the previous step, the instance ID, and the authorized time window. If the SNC Access Control plugin is enabled, the instance verifies that the user is:
   - Listed
   - Active
   - Configured to access the instance in the current time window
9. If the user is authenticated, the instance creates a synthetic user in memory with the given roles. This user does not persist after the time limit expires, the user logs off, or the instance is restarted.
Audit logging

The following logging tracks logins and activity by Customer Service and Support employees:

- Event logs: The event logs show all Customer Service and Support logins to an instance.
- Transaction logs: The transaction logs show all activity on the instance, including any efforts to delete logs.

Note: To learn more about this plugin, see SNC Access Control plugin (instance security hardening) in Instance Security Hardening Settings.

Request ServiceNow access control

You request activation of the SNC Access Control plugin (com.snc.snc_access_control).

Role required: admin

There are two ways to request a plugin:

- Access the Now Support Service Catalog directly by clicking Service Catalog > Activate Plugin on Now Support.
- Access the Now Support Service Catalog through the All Applications page on your instance by following these steps.

1. Navigate to System Applications > All Available Applications > All.
2. On the All Applications page, click **Request Plugin** to open the Request form on HI.
3. On Now Support, select the redirect link to access the Now Support Service Portal Service Catalog.

<table>
<thead>
<tr>
<th>Activate Plugin</th>
</tr>
</thead>
<tbody>
<tr>
<td>In order to enhance the user experience, we have redesigned Activate a Plugin service catalog. Please use the new Hi Service Portal 'Activate a Plugin' service catalog item. You can also use Manage Instances page on Service Portal to Activate a Plugin.</td>
</tr>
</tbody>
</table>

4. On the form, fill in the fields.

**Activate Plugin request form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Instance</td>
<td>Instance on which to activate the plugin.</td>
</tr>
<tr>
<td>Plugin Name</td>
<td>Name of the plugin to activate.</td>
</tr>
<tr>
<td>Specify the date and time you would like this plugin to be enabled</td>
<td>The date and time must be at least two business days from the current time.</td>
</tr>
</tbody>
</table>

**Note:** Plugins are activated in two batches, once in the morning and once in the evening, on every business day in the US Pacific time zone. If the plugin must be activated at a specific time, enter the request in the Reason/Comments field.

| Reason/Comments | Information that would be helpful for the ServiceNow personnel who are activating the plugin. For example, if you need the plugin activated at a specific time instead of during one of the default activation windows, specify that in the comments. |

5. Click **Submit**.

**Configure ServiceNow access control**

Configure an access control record to specify one or more Customer Service and Support employees who have permission to log in your instance.

Role required: admin

**Note:** The SNC Access Control (com.snc.snc_access_control) plugin prevents Customer Service and Support personnel from accessing the instances without your express permission. However, other authorized ServiceNow Operations personnel, in their capacity to support and manage the product, are required to perform administrative actions on the underlying infrastructure. This infrastructure includes servers and databases, among other infrastructure components that make up the SaaS solution. This access method is fully auditable and tracked.
This plugin enables you to restrict access to your instance without your express permission, so it may affect support service levels and the Availability SLA. Availability SLA is then measured from the time that Support staff personnel are granted access to your instance.

2. Click New.
3. Fill in the form fields (see table).
4. Click Submit.

### SNC Access Control

<table>
<thead>
<tr>
<th>Form fields</th>
<th>Description</th>
</tr>
</thead>
</table>
| Name        | Names each Customer Service and Support employee who has permission to log in this instance.  
  • Express the names as firstname.lastname in lower case letters, separated by a period (for example, john.smith). Each name must have a corresponding user record in hi.servicenow.com.  
  • If more than one Customer Service and Support employee has permission to log in this instance, enter multiple names and separate them by commas.  
  • To enable all Customer Service and Support employees login rights to access the instance, enter an asterisk (*) in place of the name.  
  • If you intend on restricting Customer Service and Support employee access to the instance, the values in the Name field must not have an asterisk (*) anywhere in the field. |
| Reason      | Human-readable field that describes why you are granting access permission. This field is optional. |
| Start       | Specifies the start date and time of the period during which the specified Customer Service and Support employees have login access. This field is mandatory. |
| End         | Specifies the ending date and time of the period during which the specified Customer Service and Support employees have login access. This field is mandatory. |
| Active      | Controls whether this permission record is active. The default is Active. |

### Audit logging

The following logging tracks logins and activity by ServiceNow employees.

<table>
<thead>
<tr>
<th>Event logs</th>
<th>The event logs show all ServiceNow logins to a customer instance.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction logs</td>
<td>The transaction logs show all activity on the instance, including any efforts to delete logs.</td>
</tr>
</tbody>
</table>
Access control list rules

Rules for access control lists (ACLs) restrict access to data by requiring users to pass a set of requirements before they can interact with it.

Components of ACLs

All access control list rules specify:

- The object and operation being secured
- The permissions required to access the object

The object is the target to which access needs to be controlled. Each object consists of a type and name that uniquely identifies a particular table, field, or record.

For example, all these entries specify an object:

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Object secured</th>
</tr>
</thead>
<tbody>
<tr>
<td>record</td>
<td>[incident].[-- None --]</td>
<td>The Incident table.</td>
</tr>
<tr>
<td>record</td>
<td>[incident].[active]</td>
<td>The Active field in the Incident table.</td>
</tr>
<tr>
<td>REST_Endpoint</td>
<td>user_role_inheritance</td>
<td>The record for the user_role_inheritance Scripted REST API.</td>
</tr>
</tbody>
</table>

Each operation describes a valid action the system can take on the specified object. Some objects, such as records, support multiple operations, while other objects, such as a REST_Endpoint, only support one operation.

For example, all these entries specify an operation:

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Operation</th>
<th>Operation secured</th>
</tr>
</thead>
<tbody>
<tr>
<td>record</td>
<td>[incident].[-- None --]</td>
<td>create</td>
<td>Creating records in the Incident table.</td>
</tr>
<tr>
<td>record</td>
<td>[incident].[active]</td>
<td>write</td>
<td>Updating the Active field in the Incident table.</td>
</tr>
<tr>
<td>REST_Endpoint</td>
<td>user_role_inheritance</td>
<td>execute</td>
<td>Running the user_role_inheritance scripted REST API.</td>
</tr>
</tbody>
</table>

The permissions specify when someone can access the named object and operation. Security administrators can specify permission requirements by adding:

- One or more user roles to the Requires role list.
- One or more conditions.
- A script that evaluates to true or false or sets the answer variable to true or false.

To gain access to an object and operation, a user must pass all permissions listed in an access control. For example, this access control restricts access to write operations on the incident table.
Access Control Rules allow access to the specified resource if all three of these checks evaluate to true:

1. The user has one of the roles specified in the Role list, or the list is empty.
2. Conditions in the Condition field evaluate to true, or conditions are empty.
3. The script in the Script field (advanced) evaluates to true, or sets the variable "answer" to true, or is empty.

The three checks are evaluated independently in the order displayed above.

More Info

Requires role

Role

- [ ] Bill

+ Insert a new row...

Condition

30 records match condition

Add Filter Condition  Add "OR" Clauses

Incident state ▼ is not ▼ Closed ▼ AND OR ▼

Update  Delete
To update a record in the incident table, a user must have the listed role and the record must meet the condition.

<table>
<thead>
<tr>
<th>Permission type</th>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requires role</td>
<td>Requires role: itil</td>
<td>Only allow users with the itil role to update incidents.</td>
</tr>
<tr>
<td>Condition</td>
<td>[Incident state] [is not] [Closed]</td>
<td>Only allow updates to active incident records.</td>
</tr>
</tbody>
</table>

**ACL evaluation process**

An ACL rule only grants a user access to an object if the user meets all of the permissions required by the matching ACL rule.

- The condition must evaluate to **true**.
- The script must evaluate to **true** or return an answer variable with the value of **true**.
- The user must have one of the roles in the required roles list. If the list is empty, this condition evaluates to **true**.
- [Record ACL rules only] The matching table-level and field-level ACL rules must both evaluate to **true**.
ACL evaluate permissions
Whenever a session requests data, the system searches for access control rules that match the requested object and operation. If there is a matching access control rule, then the system evaluates if the user has the permissions required to access the object and operation. If an access control rule specifies more than one permission, then the user must meet all permissions to gain access to the object and operation. Failing any one permission check prevents the user from accessing the matching object and operation.

If a user does not meet the permissions of the first matching rule, the system evaluates the permissions of the next matching access control rule as specified by the access control processing order. If the user fails to meet the permissions of any matching access control rule, the system denies access to the requested object and operation.

Note: If there are no matching access control rules for the requested object and operation, then the system grants the user access to it. In practice, it is rare for the system to find no matching rules because the system has a set of default access control rules that protect all record operations.

The effects of being denied access to an object depend on the ACL rule that the user failed. For example, failing a read operation ACL rule prevents the user from seeing the object. Depending on the object secured, the ACL rule hides a field on a form, hides rows from a list, or prevents a user from accessing a UI page. The following table contains complete list of results of failing an ACL rule for a given operation and object type.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Results of failing an ACL rule on object</th>
</tr>
</thead>
<tbody>
<tr>
<td>execute</td>
<td>User cannot execute scripts on a record or UI page.</td>
</tr>
<tr>
<td>create</td>
<td>User cannot see the <strong>New</strong> UI action from forms. The user also cannot insert records into a table using API protocols such as web services. A <strong>create</strong> ACL with a condition requiring that a field contain a specific value always evaluates as false. Fields on new records are considered empty until the record is saved.</td>
</tr>
<tr>
<td>read</td>
<td>User cannot see the object in forms or lists. The user also cannot retrieve records using API protocols such as web services.</td>
</tr>
<tr>
<td>write</td>
<td>User sees a read-only field in forms and lists, and the user cannot update records using API protocols such as web services.</td>
</tr>
<tr>
<td>delete</td>
<td>User cannot see the <strong>Delete</strong> UI action from forms. The user also cannot remove records from a table using API protocols such as web services.</td>
</tr>
<tr>
<td>edit_task_relations</td>
<td>User cannot define relationships between task tables.</td>
</tr>
<tr>
<td>edit_ci_relations</td>
<td>User cannot define relationships between Configuration Item [cmdb_ci] tables.</td>
</tr>
<tr>
<td>save_as_template</td>
<td>Used to control the fields that should be saved when a template is created.</td>
</tr>
<tr>
<td>add_to_list</td>
<td>User cannot view or personalize specific columns in the list mechanic.</td>
</tr>
<tr>
<td>list_edit</td>
<td>User cannot update records (rows) from a list.</td>
</tr>
<tr>
<td>report_on</td>
<td>User cannot create a report on the ACL table. For more information, see Restrict report creation with an ACL rule.</td>
</tr>
<tr>
<td>Operation</td>
<td>Results of failing an ACL rule on object</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>report_view</td>
<td>User cannot view the content of a report on the ACL table or on the ACL field. For more information, see Restrict report creation with an ACL rule.</td>
</tr>
<tr>
<td>personalize_choices</td>
<td>User cannot right-click a choice list field and select Configure Choices.</td>
</tr>
</tbody>
</table>

### ACL matching requirements for objects

<table>
<thead>
<tr>
<th>Object Type</th>
<th>Matching ACL Rules Required to Access Object</th>
<th>Existing Wildcard ACL Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client-callable script includes</td>
<td>Users must meet the permissions of two ACL rules:</td>
<td>By default, there are no wildcard (*) rules for these object types. If you create a wildcard ACL rule for one of these objects, then the ACL rule applies to all objects of this type.</td>
</tr>
<tr>
<td>Processors</td>
<td>1. All wildcard ACL rules for the object (if any ACL rule exists for the operation).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. The first ACL rule that matches the object's name (if any ACL rule exists for the operation).</td>
<td></td>
</tr>
<tr>
<td>UI pages</td>
<td>Users must meet the permissions of two ACL rules:</td>
<td>By default, there are wildcard table rules (<em>) for the create, read, write, and delete operations and wildcard field rules (</em>.*) for the personalize_choices, create, and save_as_template operations. When you create a new table, create new ACL rules for the table unless you want to use the provided wildcard ACL rules.</td>
</tr>
<tr>
<td>Record</td>
<td>1. The first ACL rule that matches the record's field (if any ACL rule exists for the operation).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. The first ACL rule that matches the record's table (if any ACL rule exists for the operation).</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** The Security manager default behavior (`glide.sm.default_mode`) property determines whether users can access objects that only match against wildcard table ACL rules. When this property is set to **Deny access**, only administrators can access objects that match the wildcard table ACL rules.

**Note:** The wildcard field ACL rule (".*") for the create operation reuses the same permissions as the write operation. This means that the create permissions are the same as the write permissions unless you define an explicit create operation ACL rule.

### Multiple ACL rules at the same point in the processing order

If two or more rules match at the same point in the processing order, the user must pass any one of the ACL rules permissions to access the object. For example, if you create two field ACL rules for `incident.number`, then a user who passes one rule has access to the number field regardless of whether the user failed any other field ACL rule at the same point in the processing order.
Required role

Normal admin users can view and debug access control rules. However, to create or update existing access control rules, administrators must elevate privileges to the security_admin role. See Elevate to a privileged role for instructions.

ACL rules in scoped applications

You can create ACL rules for objects in the same scope as the ACL rule and for tables with at least one field that is in the same scope as the ACL rule.

For tables that are in a different scope than the ACL rule record, the types of rules are limited.

- You can create an ACL rule for any table, UI page, or other object that is in the same scope as the ACL rule.
- You can create an ACL for a field that is in the same scope as the ACL rule.
  - If the table is in the same scope, you can use a script to evaluate permissions.
  - If the table is in a different scope, you cannot use a script to evaluate permissions.
- You cannot create or modify ACL rules for objects that are in a different scope than the application you have selected in the application picker, including adding a role to an ACL in a different scope.
- You can create wildcard table rules (*) only in the global scope.
- You can create wildcard field rules (*) only for tables in the same scope as the ACL rule.

ACL rule types

Create ACL rules on different components of the system.

Record ACL rules

Record ACL rules consist of table and field names.

- The table name is the table that you want to secure. If other tables extend from this table, then the table is considered a parent table. ACL rules for parent tables apply to any table that extends the parent table.
- The field name is the field that you want to secure. Some fields are part of multiple tables because of table extension. ACL rules for fields in a parent table apply to any table that extends the parent table.

ACL rules can secure the following record operations:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>create</td>
<td>Enables users to insert new records (rows) into a table.</td>
</tr>
<tr>
<td>read</td>
<td>Enables users to display records from a table.</td>
</tr>
<tr>
<td>write</td>
<td>Enables users to update records in a table.</td>
</tr>
<tr>
<td>delete</td>
<td>Enables users to remove records from a table or drop a table.</td>
</tr>
<tr>
<td>edit_task_relations</td>
<td>Enables users to extend the Task [task] table.</td>
</tr>
<tr>
<td>edit_ci_relations</td>
<td>Enables users to extend the Configuration Item [cmdb_ci] table.</td>
</tr>
<tr>
<td>save_as_template</td>
<td>Enables users to save a record as a template.</td>
</tr>
<tr>
<td>Operation</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>add_to_list</td>
<td>Prevents users from viewing or personalizing specific columns in the list mechanic.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Note: Conditions and scripts are not supported." /></td>
</tr>
<tr>
<td>list_edit</td>
<td>Enables users to update records (rows) from a list.</td>
</tr>
<tr>
<td>report_on</td>
<td>Enables users to report on tables. This operation is also valid for field ACL rules.</td>
</tr>
<tr>
<td>personalize_choices</td>
<td>Enables users to configure the table or field.</td>
</tr>
</tbody>
</table>

Record ACL rules are processed in the following order:

- Match the object against table ACL rules.
- Match the object against field ACL rules.

This processing order ensures that users gain access to more general objects before gaining access to more specific objects. A user must pass both table and field ACL rules to access a record object.

- If a user fails a table ACL rule, the user is denied access to all fields in the table, even if the user passes a field ACL rule.
- If a user passes a table ACL rule, but fails a field ACL rule, the user cannot access the field described by the field ACL rule.
Start
User requests access to a record object

Find ACL rules matching object

1. ACL name matches table?
2. ACL name matches parent table?
3. ACL name matches *?

Find first matching table ACL rule

Match found

No matches

1. ACL name matches table.field?
2. ACL name matches parent table.field?
3. ACL name matches *.*?
4. ACL name matches table.*?
5. ACL name matches parent table.*?
6. ACL name matches *.*?

Find first matching field ACL rule

Pass
Evaluate ACL permissions

Match found

Fail
Evaluate ACL permissions

No matches
Grant user access to the record object

Pass

Deny user access to the record object

End
Processor ACL rules

Processor ACL rules specify the processor you want to secure. For a list of available processors, navigate to System Definition > Processors.

By default, an ACL rule for the EmailClientProcessor is included to restrict the email client to users with the itil role. Processor ACL rules honor the STAR (*) rule if they cannot find a more specific ACL for those resources.

Table ACL rules

The user must first pass the table ACL rule. Since the base system includes STAR (*) table ACL rules that match every table, the user must always pass at least one table ACL rule. The base system provides additional table ACL rules to control access to specific tables.

Table ACL rules are processed in the following order:
1. Match the table name. For example, incident.
2. Match the parent table name. For example, task.
3. Match any table name (*). For example, *.

If a user fails all table ACL rules, the user cannot access the fields in any table. If a user passes a table ACL rule, the system then evaluates the field ACL rules.

Field ACL rules

After a user passes a table ACL rule, field ACL rules are processed in the following order:
1. Match the table and field name. For example, incident.number.
2. Match the parent table and field name. For example, task.number.
3. Match any table (*) and field name. For example, *.number.
4. Match the table and any field (*). For example, incident.*.
5. Match the parent table and any field (*). For example, task.*.
6. Match any table (*) and any field (*). For example, *.*.

A user must pass the table ACL rule to be granted access to the table's fields. For example, the user must first pass the table ACL rule for the incident table to access the Number field in the incident table.

The first successful field ACL evaluation stops ACL rule processing at the field level. When a user passes a field ACL rule, the system stops searching for other matching field ACL rules. For example, if a user passes the field ACL rule for incident.number, the system stops searching for other ACL rules that secure the Number field in the incident table.

UI page ACL rules

UI page ACL rules specify the UI page to be secured. For a list of available UI pages, navigate to System UI > UI Pages. When defining an ACL rule for a UI page, use the fully scoped page name. For example, x_myapp_mypage.
Note: You can use the STAR (*) character in the Name field on ui_page type ACLs to match any UI pages.

UI page ACL rules honor the STAR (*) rule if they cannot find a more specific ACL for those resources. For example, if you have a UI page named mysecretpage but do not define an ACL for this UI page, the STAR (*) rule for the UI page processor is used for access check.

ACL rules can secure the following UI page operation:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>read</td>
<td>Allows users to display the UI page.</td>
</tr>
</tbody>
</table>

Client-callable script include ACL rules

Script include ACL rules specify the client-callable script include to be secured. For a list of available script includes, navigate to System Definition > Script Includes. You can personalize the list to show the Client callable column.

The base system does not include any ACL rules for client-callable script includes.

Client-callable script include ACL rules honor the STAR (*) rule if they cannot find a more specific ACL for those resources.

ACL control of function fields

When evaluating access to a function field, in addition to checking access to the function field itself, the system also checks access to the function's contributing fields. Contributing fields are those used as the arguments in a given function definition.

For more information about function fields, see Function field.

In Paris and earlier, the system simply checks access to the function field itself (as with any other field). If the ACLs on that field allow access, the user receives the resulting value, regardless of whether the user has access to the contributing fields.

In Quebec, the system also requires access to all contributing fields in order to allow access to the function field. If one or more of the contributing field ACLs refuse access, the function field also refuses access.

The only operations affected by the new requirement are read and report_view. Report_view has its own additional requirements.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>read operation</td>
<td>A user has read access to a function field only if both of the following are true:</td>
</tr>
<tr>
<td></td>
<td>• The user has read access to the function field.</td>
</tr>
<tr>
<td></td>
<td>• The user has read access to all of the contributing fields used in the function.</td>
</tr>
</tbody>
</table>
### Operation Description

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
</table>
| report_view operation | A user has report_view access to a function field only if all of the following are true:  
  - The user has report_view access to the function field.  
  - The user has report_view access to each of the contributing fields.  
  - There is a role-only ACL without conditions and without a script, and the user has that role.  
  - The user has role-only read access to the contributing fields, such that only ACLs without condition or script can allow. |

### Examples

**Given:**
- Table: salary
- Columns: base, bonus, total (all are Integers in this example)
- Function field: The total column is marked as a function field, with function definition `glidefunction:add(base, bonus)`.
- Contributing fields: base and bonus, since they're used in the function definition
- Roles: salary_admin, bonus_admin

**Example 1: All fields allow access**

<table>
<thead>
<tr>
<th>ACLs</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>total, base, bonus: read and report_view for role salary_admin, with no conditions or scripts</td>
<td>A user with the salary_admin role is granted read and report_view access to total because they have the required role.</td>
</tr>
</tbody>
</table>

**Example 2: Contributing field refuses read access**

<table>
<thead>
<tr>
<th>ACLs</th>
<th>Result</th>
</tr>
</thead>
</table>
| total, base: read and report_view for role salary_admin, with no conditions or scripts  
  bonus: report_view for role salary_admin, with no conditions or scripts  
  bonus: read for role bonus_admin, with no conditions or scripts | A user with the salary_admin role is refused read and report_view access to total, because bonus refuses read access to their role. |
Example 3: Contributing field ACL has script

<table>
<thead>
<tr>
<th>ACLs</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>total, base: read and report_view for role salary_admin, with no conditions or scripts</td>
<td>A user with the salary_admin role is granted read access to total, because they have the required role for all fields. But the same user with the salary_admin is refused report_view access, because the read ACL with the script refuses access by default for this case, even though they have the required role.</td>
</tr>
<tr>
<td>bonus: report_view for role bonus_admin, with no conditions or scripts</td>
<td></td>
</tr>
<tr>
<td>bonus: read for role salary_admin, with a script (note that it doesn’t matter what’s in the script, only that it’s there)</td>
<td></td>
</tr>
</tbody>
</table>

Create an ACL rule

Create a custom ACL rule to secure access to new objects or to change the default security behavior.

Role required: security_admin

To create ACL rules, you must elevate privileges to the security_admin role. For tables that are in a different scope from the ACL rule record, the types of rules are limited.

1. Elevate privileges to the security_admin role.
3. Click New.
4. Complete the form.

Access control fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select what kind of object this ACL rule secures. The type of object determines how the object is named and what operations are available. This field becomes read only after the ACL rule is created. If you want to change the type, you must delete the ACL and create a new one with the correct type.</td>
</tr>
<tr>
<td>Operation</td>
<td>Select the operation this ACL rule secures. Each object type has its own list of operations. An ACL rule can only secure one operation. To secure multiple operations, create a separate ACL rule for each.</td>
</tr>
<tr>
<td>Admin overrides</td>
<td>Select this check box to have users with the admin role automatically pass the permissions check for this ACL rule. Admin users pass regardless of what script or role restrictions apply. However, the nobody role, which only ServiceNow personnel can assign, takes precedence over the admin override option. If an ACL is assigned the nobody role, admin users cannot access the resource even when Admin overrides is selected. See Base system roles. Clear this check box if administrators must meet the permissions defined in this ACL rule to gain access to the secured object. Since administrators always pass role checks (see the description of the Requires role field), use the condition builder or Script field to create a permissions check that administrators must pass.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Active</td>
<td>Select this check box to enforce this ACL rule.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Select this check box to display the <strong>Script</strong> field.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the object being secured, either the record name or the table and field names. The more specific the name, the more specific the ACL rule. You can use the wildcard character asterisk (<em>) in place of a record, table, or field name to select all objects that match a record type, all tables, or all fields. You cannot combine a wildcard character and a text search. For example, inc</em> is not a valid ACL rule name, but incident.* and *.number are valid ACL rule names. <strong>Note:</strong> Click the blue triangle to manually enter the record name or the table and field names of the object being secured. Use this option to secure an object that does not appear in the dropdown.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the object or permissions this ACL rule secures.</td>
</tr>
<tr>
<td>Requires role</td>
<td>Use this list to specify the roles a user must have to access the object. If you list multiple roles, a user with any one of the listed roles can access the object. The Requires role list appears as a related list. <strong>Note:</strong> Users with the admin role always pass this permissions check because the admin role automatically grants users all other roles.</td>
</tr>
<tr>
<td>Condition</td>
<td>Use this condition builder to select the fields and values that must be true for users to access the object.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Script | Enter a custom script describing the permissions required to access the object. The script can use the values of the current and previous global variables as well as system properties. The script must generate a true or false response in one of two ways:  
  - return an answer variable set to a value of true or false  
  - evaluate to true or false  
  In either case, users only gain access to the object when the script evaluates to true and the user meets any conditions the ACL rule has. Both the conditions and the script must evaluate to true for a user to access the object.  
  
  **Note:** If the evaluated item is in a related list, current points to the item the related list is on, not to the current item the ACL is for. However, If the item you are evaluating the ACL for is not in a related list, current points to the actual item. |
5. Right-click the form header and select **Save**.
Secure records in an embedded list

To apply security to the records in embedded lists, limit editing and deleting records in embedded lists to specific roles.

Role required: security_admin

1. Navigate to **System Security > Access Control (ACL).**
2. Open the **Write** or **Delete** record for the appropriate table.
3. In the Requires Role section of the form, add the roles that have write or delete permission for that table.
4. Save the changes.

   When records from the associated table appear in an embedded list, the edit and delete options are available only to users with the specified roles.

**Contextual Security Manager**

Contextual Security Manager protects your data by controlling read, write, create, and delete authorization.

**Key advantages**

The Contextual Security Manager is aware of the system table hierarchy, enabling you to create specific security rules for a field based on where in the hierarchy it is displayed. Benefits of the Contextual Security Manager include:

- **Contextual security**: Secure a record based on the contents of the record.
- **Hierarchical security**: Apply security rules to any level in the object hierarchy.

**Securing fields and tables**

With the legacy Simple Security Manager, you could secure fields and tables by adding roles to the appropriate dictionary entry. With the Contextual Security Manager, these dictionary roles are no longer tested. Instead, the system looks for ACL rules on fields and tables.

**Warning:** After you install the Contextual Security Manager, you must secure fields and tables via ACL rules. Even if you configure the dictionary form and add roles to a dictionary entry, no change in rights occurs.

**Contextual security and roles**

You can grant roles to users or groups. However, after installing the Contextual Security Manager, the roles field on the user record is no longer checked and no longer appears on your user and group forms. Instead, you must add roles to the Roles related list instead of to the user or group record.

Applications and modules contain lists of the roles required to view them. For example, to view the System Definition application, the admin role is required. Security rights for applications and modules are still defined using role arrays.

Both catalog items and catalog variables contain lists of the roles required to view them. Security rights for catalog items and catalog variables are still defined via these role arrays.

Under the Contextual Security Manager, a group still automatically inherits any role granted to the group when the inherits flag for the role is set to true.
Activating the Contextual Security Manager

The Contextual Security Manager is active in the base system. If there are many duplicate entries in the User Roles table, you may need to upgrade to Contextual Security: Role Management V2 to eliminate duplicate roles. Plugins include:

**Contextual Security: Role Management [com.glide.role_management]**

Provides contextual security functionality. This plugin is automatically installed.

**Contextual Security: Role Management V2 [com.glide.role_management.inh_count]**

Prevents duplicate entries caused by inherited roles in the User Roles [sys_user_has_role] table. This plugin is automatically installed on new instances and can be activated for upgrades. The Contextual Security: Role Management Enhancements plugin is a previous version of this plugin. The Role Management Enhancements plugin does not include the RoleManagementVerify() script. This script returns a list of changes that an upgrade will perform, enabling you to monitor changes made by the plugin.

**Note:** After activating Role Management V2, you must set the glide.role_management.v2.audit_roles system property to allow the Audit Roles table to create audit records related to user roles. To learn more about setting this property and about the Audit Roles table, see:

- Enable role auditing with Contextual Security: Role Management V2.
- Contextual Security: Role Management plugin (instance security hardening) in Instance Security Hardening Settings.
- Audit user roles

Prevent duplicate entries with Contextual Security: Role Management V2

Roles inherited from other roles are added as individual entries in the User Roles table [sys_user_has_role], potentially causing one role to have duplicate entries. Contextual Security: Role Management V2 eliminates these duplicate entries and prevents future duplicates.

Eliminate duplicate entries through inheritance count

Contextual Security: Role Management V2 uses the Inheritance Count (inh_count) column to track the number of times a role is inherited from another role or group. In the User Roles [sys_user_has_role] table, a user can inherit a specific role only one time, eliminating duplicate entries. The Inheritance Count (inh_count) column is read-only and calculates the number of times the user inherits a role.

Activation changes

Contextual Security: Role Management V2 is automatically installed on new instances and can be activated for upgrades. When activated, Contextual Security: Role Management V2 replaces both Contextual Security and Contextual Security: Role Management Enhancements.

When Contextual Security: Role Management V2 is activated, the following columns are deprecated, but remain in the User Roles table for backward compatibility:

- granted_by (used only by Role Delegation)
- included_in_role
- included_in_role_instance
CAUTION: If these columns are in use in any custom scripts on your instance, do not upgrade to Role Management V2.

Visualize role inheritance through the Role Inheritance Map

The Role Inheritance Map displays a visual representation of inherited roles. You can use this map to understand the roles represented in the Inheritance Count (inh_count) column. To view the Role Inheritance Map, configure the User Roles [sys_user_has_role] table to display the Role Inheritance Map column.

Role Inheritance Map

Upgrade to Contextual Security: Role Management V2

Contextual Security: Role Management V2 is automatically installed on new instances. You can upgrade from Contextual Security: Role Management to Contextual Security: Role Management V2 to eliminate duplicate roles in the User Roles table and prevent future duplicates.

Role required: admin, security_admin

You must have the admin role and Elevate to a privileged role to obtain the effective security_admin role.

Note: Before upgrading to Contextual Security: Role: Management V2, you must enable the Audit Roles table to create audit records related to user roles. To learn more about setting the required system property, see Enable role auditing with Contextual Security: Role Management V2.

This procedure describes how to upgrade your Contextual Security role and how to activate the related plugins described in the following table.
Plugins for Contextual Security: Role Management V2

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contextual Security: Role Management V2 [com.glide.role_management.inh_count]</td>
<td>Prevents duplicate entries in the User Roles [sys_user_has_role] table.</td>
</tr>
</tbody>
</table>

Before upgrading from Contextual Security: Role Management to Contextual Security: Role Management V2, test the results of an upgrade by running the script. The script returns a list of changes that an upgrade will perform. If the changes are acceptable, install the Contextual Security: Role Management V2 plugin. If the changes are not acceptable, do not install the Contextual Security: Role Management V2 plugin. Alternatively, you can perform the upgrade and then manually make any necessary changes.

1. Test the impact of an upgrade prior to upgrading by running the following script.
   a) Navigate to System Definition > Scripts - Background.
   b) Run the following script in global scope:

   ```java
   new RoleManagementVerify().verifyInheritedRoles();
   ```

   For large sys_user_has_role tables, the execution may take up to several hours to complete. Do not edit or add user roles during this time.

   Example result based on test data:

   ```
   *** Script: 2016-12-01 19:58:54 Starting checking of inherited roles for all users...
   *** Script: User: itam, inherited roles to be ADDED: financial_mgmt_user
   *** Script: User: bernard.laboy, inherited roles to be DELETED: api_analytics_read, pa_viewer, rest_api_explorer, a123
   *** Script: User: bernard.laboy, inherited roles to be ADDED: dependency_views
   *** Script: Number of inherited-role records in sys_user_has_role, current: 260, after re-calculation: 258
   *** Script: Number of users with discrepancies for inherited roles: 2
   *** Script: 2016-12-01 19:58:55 Finished checking of inherited roles for all users!
   ```
   c) Evaluate the script results to determine whether the proposed changes are acceptable.

2. Activate the Contextual Security: Role Management V2 plugin.
   a) Navigate to System Definition > Plugins.
   b) Find and click the plugin name.
   c) On the System Plugin form, review the plugin details and then click the Activate/Upgrade related link.
   d) Click Activate.

After activating Role Management V2, the changes outlined in the script result are enacted. The Inheritance Count (inh_count) column in the User Roles table is read-only and automatically reflects the number of times the user inherits a role.
Enable role auditing with Contextual Security: Role Management V2

Set a system property to enable the Audit Roles table to create audit records related to user roles.

Role required: admin

When enabled, the Audit Roles [sys_audit_role] table maintains changes to user records. For more information about role audits, see Audit user roles. If the Contextual Security: Role Management V2 [com.glide.role_management.inh_count] plugin is installed, you must set a system property to `true` to enable role auditing.

2. Add the `glide.role_management.v2.audit_roles` system property and set it to `true`.

   If the Contextual Security: Role Management V2 [com.glide.role_management.inh_count] plugin is installed, setting this property to `true` enables the Audit Roles [sys_audit_role] table to create records when user roles change.

Double-check form submission

When the system determines that a particular field (such as task.number) should not be written to by the current user, the system renders that field in a read-only mode, which is why the number field is not writable on most incidents.

If you set the system to double-check the values of any incoming fields for writability, then the system applies the same set of security rules to the inbound leg of a transaction. When you submit an incident, for example, the system double-checks to determine if the number field can be written to before posting any changes.

If you tell the system not to double-check inbound transactions, then the system allows you to write to a nominally read-only field if that is the transaction the client sends back. In many deployments this is actually a desirable behavior if, for example, you are using client scripts to set nominally read-only fields in response to user selections in other, writable fields.

<table>
<thead>
<tr>
<th>Property</th>
<th>Location</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Double check security on inbound transactions during form submission (rights are always checked on form generation)</td>
<td>System Properties &gt; Security</td>
<td>Disabled (no double-checking)</td>
</tr>
</tbody>
</table>

Default deny property

The default deny property (`glide.sm.default_mode`) controls the security manager default behavior when the only matching ACL rules are the wildcard table ACL rules.

A set of wildcard table ACL rules for the most common record-based operations are available: read, write, create, and delete. A significant number of ACLs to provide role-based access to system tables are also available. For example, there are ACLs that grant `sys_script` access to the `business_rule_admin` role because that role is documented as being able to manage business rules.

Use the `glide.sm.default_mode` property to deny or allow these operations on all tables:

- **Deny Access**: The wildcard table ACL rules restrict the read, write, create, and delete operations on all tables unless the user has the admin role or meets the requirements of another table ACL rule. Other operations, such as `report_on` and `personalize_choices`, are unaffected by this setting.
- **Allow Access**: The wildcard table ACL rules allow the read, write, create, and delete operations on all tables unless there are specific table ACL rules in place to restrict such operations.

You cannot reset `glide.sm.default_mode` to Allow Access once it has been set to Deny Access.
**Note:** By default, the wildcard table ACL rules are the only ACL rules that check for the value of the `glide.sm.default_mode` property. If you want to control other operations with this setting, create your own ACL rules to check for this property value. To learn more about this property, see Default deny (instance security hardening) in Instance Security Hardening Settings.

### Advanced ACL configuration

In addition to creating new ACLs or modifying existing ones, you can configure other aspects of ACL functionality.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply ACL script conditions to reference fields</td>
<td>Enable a property to allow script conditions to apply to reference fields if you want to control access to the data that a reference field displays on a form or in a list. There might be an impact to the performance of your instance if you enable this.</td>
</tr>
<tr>
<td>Apply ACLs to AJAXGlideRecord (client-side Glide record)</td>
<td>Apply ACLs to GlideAjax API calls so that the system queries only the data that the currently connected user has rights to access.</td>
</tr>
<tr>
<td>Evaluate the admin override at the access level</td>
<td>Force ACL evaluation for admin overrides at the access level. By default, users with the admin role automatically pass the permissions check for this ACL rule when the Admin Overrides option is selected on the ACL rules form.</td>
</tr>
<tr>
<td>Use ACL debugging and troubleshooting tools</td>
<td>Use tools like the ACL watcher, field level debugging, and access ACL rule output messages to help you troubleshoot and debug ACLs.</td>
</tr>
</tbody>
</table>

### Provide external users access to a table

To enable users with only the `snc_external` role to access the list view of a table, you must create a series of ACLs.

Role required: security_admin

1. **Elevate to the security_admin role.**
2. **Create a new ACL with the following settings:**
   - **Type:** `ui_page`
   - **Operation:** `read`
   - **Name:** `{table_name}_list`
   - **Required role:** `snc_external`

3. On the default `read` ACL for the table, add `snc_external` in the Required role list. Create the ACL if it does not already exist.
4. **Use these settings to create another ACL:**
   - **Type:** `ui_page`
   - **Operation:** `read`
   - **Name:** `{table_name}`
   - **Required role:** `snc_external`
5. Use these settings to create another ACL to give the user write access to a field in the table:

- **Type**: record
- **Operation**: create
- **Name**: `{table_name} {column_name}`
- **Required role**: snc_external

Repeat this step for every field that you want to give the user write access to. Use an asterisk (*) instead of the column name to provide access to all fields at once.

**Apply ACL script conditions to reference fields**

If you want to enable script conditions for reference fields, you can add a system property. The default behavior is intended to improve instance performance. If you want to enable script conditions for reference fields, add the following system property.

**System property**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.sys_reference_row_check</td>
<td>Controls whether the script conditions of Access Control Rules apply to a table's reference fields.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: <strong>false</strong></td>
</tr>
<tr>
<td></td>
<td>• Location: Add to the System Properties [sys_properties] table</td>
</tr>
</tbody>
</table>

**Apply ACLs to AJAXGlideRecord (client-side Glide record)**

From within client scripts, it is possible to query arbitrary data from the server via the AJAXGlideRecord (renamed GlideAjax) API, by using syntax similar to a server-side glide record. This is an extremely powerful and useful tool in many deployments. You can set a system property to perform ACL validation when server-side records (for example, tables) are accessed using GlideAjax APIs within a client script.

If you choose to apply access control lists (ACL) to GlideAjax API calls, then you can only query data to which the currently connected user has rights to access. For example, if the user is logged in as an ESS user who has no rights to read the cmn_location table, then any GlideAjax API call by the user will fail.

If you run the system without an ACL checking on GlideAjax calls, then the API can return information that the currently logged in user could not otherwise access via the UI.

**Note:** Set this property in **System Properties > Security**.

<table>
<thead>
<tr>
<th>Property</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply standard security ACLs to AJAXGlideRecord calls</td>
<td>ACL checking enforced</td>
</tr>
</tbody>
</table>

**Note:**

To learn more about this property, see Enabling AJAXGlideRecord ACL checking (instance security hardening) in Instance Security Hardening Settings.
Evaluate the admin override at the access level

If you want to force ACL evaluation for admin overrides at the access level, you can add a system property.

Role required: security_admin

ACLs are evaluated cumulatively. If there are number of ACLs on any given field and the Admin Overrides option is false (not selected) on one of them, then the effective admin overrides for all the ACLs are considered to be false. This causes admins to be unable to pass even the ACL where the override should be in effect.

- Add the following property to the system properties table:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.security.admin.override.accessterm</td>
<td>Evaluates the admin override condition at the access term level.</td>
</tr>
<tr>
<td></td>
<td>- Type: true</td>
</tr>
<tr>
<td></td>
<td>- Default value: true for new instances, false for upgrades</td>
</tr>
<tr>
<td></td>
<td>- Location: Add to the System Properties [sys_properties] table</td>
</tr>
</tbody>
</table>

ACL debugging tools

Field level debugging and access ACL rule output messages are available to help you troubleshoot and debug ACLs. The ACL configuration watcher lets you know what related ACLs exist when you modify one.

Field level debugging

When debugging is enabled, a small bug icon (#) appears beside each field with an ACL rule. Clicking the icon lists the ACL rules that apply for the field and the evaluation results.

Field level security on an incident

After enabling ACL debugging, you can impersonate another user to see what ACL rules the user passes and fails. When you impersonate a user, you can only see what that user is allowed to see. For example, you cannot view a record that an ACL prevents the user from seeing. To make debugging easier, read-only access to certain ACL-related tables is enabled by default, even when impersonating a user that does not have read access to the tables. To change this functionality, set the following property to false.

To enable ACL rule debugging, navigate to System Security > Debug Security Rules.
<table>
<thead>
<tr>
<th>System property</th>
<th>Description</th>
<th>Default setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.security.access_acl_as_impersonator</td>
<td>Allows read access to the following tables while impersonating a user: sys_security_acl, sys_security_operation, sys_security_type, and sys_user_role. As a result, the impersonating user can read data that the impersonated user cannot read.</td>
<td>true</td>
</tr>
</tbody>
</table>

**Note:** When the property is set to false, the impersonated user might be prevented from reading ACL-related data. In this case, a second session logged in as admin or security_admin might be required to debug ACLs.

### ACL rule output messages

ACL debugging displays ACL rule output messages at the bottom of each list and form. The output message displays the following:

<table>
<thead>
<tr>
<th>Message element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TIME</td>
<td>The total time used to process this ACL rule.</td>
</tr>
<tr>
<td>PATH</td>
<td>Information that uniquely identifies each ACL rule in the format: &lt;ACL rule type&gt;/&lt;ACL rule name&gt;/Operation.</td>
</tr>
<tr>
<td>CONTEXT</td>
<td>The object being evaluated by the ACL rule.</td>
</tr>
<tr>
<td>RC</td>
<td>The return code of the ACL rule. A true value passes the ACL rule. A false value fails the ACL rule.</td>
</tr>
</tbody>
</table>
| RULE            | A brief summary of processors and scripts, followed by ACL results for each table-level and field-level ACL evaluation. Most ACL evaluations show an overall pass or fail result followed by a breakdown of the results for each type of ACL criteria:  
  - iAccessHandler: An internal system check using hidden source code on the platform. This is a system security check that you cannot modify. IAccessHandler can grant or deny access to a resource without evaluating ACLs. If IAccessHandler is ignored, then the ACLs are evaluated. You cannot modify the IAccessHandler checks in any way. For example, an IAccessHandler implementation is used for access checks on application resources and this cannot be changed. This is available starting with the Istanbul release.  
  - Roles: Verification that the user has the correct role.  
  - Condition: Verification that the user passed the condition specified on the ACL rule (if any).  
  - Script: Verification that the user passed the script specified on the ACL rule (if any). |
The icons that appear show how the ACL was evaluated:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A green checkmark (✔️)</td>
<td>Indicates the table or field passed the criteria.</td>
</tr>
<tr>
<td>A red x icon (❌)</td>
<td>Indicates the table or field did not pass.</td>
</tr>
<tr>
<td>An empty gray circle icon (〇)</td>
<td>Indicates the ACL evaluation did not need to be performed.</td>
</tr>
<tr>
<td>A blue checkmark, x, or empty circle</td>
<td>Indicates that the ACL was taken from a cached result of a previous ACL check. The icons mean the same as the above.</td>
</tr>
</tbody>
</table>

You can perform these actions on the ACL debug output:

- Select or clear these check boxes at the top of the debug output:
  - **Security rules**: Show or hide the results of the ACL checks.
  - **Others**: Show or hide other warnings or messages.

- Click the name of the ACL next to any of the output messages to open that ACL record.

- Hover the cursor over any of the icons for the four ACL checks to see more information.

**ACL troubleshooting reference**

A list of common ACL rule errors and their solutions.

Enable debugging to help troubleshoot an issue.

<table>
<thead>
<tr>
<th>Error or symptom</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>You cannot access records from a custom table.</td>
<td>Create a table ACL rule for the custom table granting users access to the table. Without an explicit table ACL rule, users must pass the permissions in the table wildcard (*) ACL rule, which by default restricts access to administrators only. Enable debugging and determine what ACL rules are evaluated for the custom table.</td>
</tr>
</tbody>
</table>
Error or symptom | Solution
---|---
You create a custom ACL rule that does not work properly. | The most likely problems are that another rule takes precedence over your custom rule in the processing order or that the user does not meet all the permission requirements for the object type. Enable debugging and verify that the ACL rule is being evaluated.

Your field ACL rule does not work properly. | There is likely a table ACL rule that the user has not met. Enable debugging and determine what ACL rules are evaluated for the field. Verify that there is not a conflicting table ACL rule or duplicate field ACL rule.

Your table ACL rule does not work properly. | There is either an ACL rule higher in the processing order or a duplicate table ACL rule interfering with the table ACL rule. Enable debugging and determine what ACL rules are evaluated for the table.

You can see a field in a list but not in form. | It is possible that the ACL rule conditions or script are being triggered in the list but not in the form. Enable debugging and determine when the ACL rules evaluate to true. Update the conditions or script to have the same behavior on the list and form.

You receive an error message when trying to execute a processor or client-callable script include. | There is an ACL rule for the processor or client-callable script include that the user has not met. If the user should have access to the object, enable debugging and determine what ACL rules are evaluated for the processor or script include. Update the ACL rule or the user roles as needed to access the object.

---

**ACL configuration watcher**

The ACL configuration watcher lets you know what related ACLs exist on a table when you insert, update, or delete an ACL on the same table.

The ACL configuration watcher is an interceptor window that displays every time you make important changes on the Access Control [sys_security_acl] table. It displays a security rules summary window where you can view ACLs related to the one you are modifying. You cannot modify any ACLs from the security rules window. To make any modifications, close the watcher window and go to those ACLs.

The ACL configuration watcher does not appear in the following situations:

- If you save or update an ACL record without actually making any changes.
- If you make minor updates (not an insert or delete), such as updating scripts, conditions, and the admin-overrides option.
- If the ACL record is not active.

**ACL Security Rules window**

The configuration watcher shows the ACL execution plan. The execution plan is displayed in the security rules pop-up window. You can view this kind of information:

**ACL configuration window elements**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>red highlight</td>
<td>An ACL that is deleted or deactivated.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>blue highlight</td>
<td>An ACL that is modified.</td>
</tr>
<tr>
<td>green highlight</td>
<td>An ACL that is added or becomes active.</td>
</tr>
<tr>
<td>Masked</td>
<td>An ACL that was effective until you made a change.</td>
</tr>
<tr>
<td>Unmasked</td>
<td>An ACL that was just made effective when you made a change.</td>
</tr>
</tbody>
</table>

**Verify Security Rules for "vtb_task.short_description"**

**Configuration watcher example**

Show ACL execution plan
Administrators can view how ACLs relate to each other by viewing an execution plan for any ACL in the instance.
Role required: security_admin

1. Elevate to a privileged role.
2. Open an ACL that is a record-type ACL.
3. Click **Show ACL Execution Plan**.

The security rules window appears for the ACL.

<table>
<thead>
<tr>
<th>Security Rules for &quot;vtb_task.description&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Write</strong></td>
</tr>
<tr>
<td>Row level</td>
</tr>
<tr>
<td>Field level</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

4. Click **Show all** to show all related ACLs, including those ACLs that are overridden and generic ACLs that apply to all records. Overridden ACLs have a line through the name, and generic ACLs have the wildcard character asterisk (*) for the name.

5. Click **Show Effective** to show only the immediate ACLs related to the one you are viewing. This action hides the ACLs on tables from which the ACL table is extended and the generic wildcard (*) ACLs.

Use the ACL configuration watcher

Use the ACL configuration watcher after you elevate to security_admin role.

Role required: security_admin

Elevate to a privileged role

1. Open an ACL that is a record-type ACL.
2. Perform an action on the ACL, such as modifying it, or selecting an option from the context menu like **Insert**.
3. If you modified any values on the Access Control form, right-click the header and select **Save** or click **Update** or **Delete**.

The Security Rules window appears. The system did not yet perform the database action on the ACL, so the changes are not yet saved.

These are examples of security rules on the Visual Task Board application's Private Task [vtb_task] table. See **ACL configuration watcher** for a description of the items on this window.
4. Just as with the execution plan, you can click **Show all** to show all related ACLs, including those that are overridden and generic ACLs that apply to all records, or click **Show Effective** to show only the immediate ACLs related to the one you are viewing.

5. Hover your mouse over any of the ACLs to see a description.

### Explicit Roles

You can give both internal users and external users access to your instance. However, you might not want both types of users to have the same level of access. To provide added security, every user must have at least one role so that the instance can distinguish between internal and external users.

As of the release, no user can have both of the explicit roles (snc_internal and snc_external). Groups and role containment cannot include both roles, either, since that would cause any group member or user who is assigned to such a group or such a role to automatically have both roles. The aborts any operation that would create such a scenario.

External users must obtain, at minimum, the snc_external role. The snc_external role indicates that the user is external to your organization. They should not have any access to resources unless explicitly allowed through ACLs for the snc_external role or additional roles that inherit the snc_external role. By default, users with the snc_external role cannot access:

- Scripted REST API resources that are not marked external.
- Tables without the role that inherits the snc_external role or the public role.
- Non-record type resources, such as processors and UI pages without the snc_external role or a role that inherits the snc_external role.
- dashboards.

Do not mark the snc_internal role as elevated. Otherwise, internal users cannot access the instance.

**Note:** You can set up encryption contexts with the snc_internal and snc_external roles. However, adding encryption contexts to more detailed roles is recommended. For more information, see .

### Explicit Roles plugin

When the Explicit Roles plugin is activated:

- All users must have the snc_internal role to access internal resources or the snc_external role to access external resources. Users without either explicit role can access only public resources.
- All existing users are automatically assigned the snc_internal role. This role does not change existing access levels or system behavior. Instead, it provides a category to differentiate internal users from external users. All internal users maintain the same level of access as before the plugin was activated.

**Tip:** To prevent changing existing functionality for users, activating the Explicit Roles plugin assigns the snc_internal user role to all existing users in the instance. This includes any external users added before
the Explicit Roles plugin was activated. After the Explicit Roles plugin is activated, do the following for all external users added before the Explicit Roles plugin was activated:

• Remove the snc_internal role.
• Add the snc_external role.

Doing the preceding ensures that external users added before activating the Explicit Roles plugin do not have access to internal resources that should be available only to internal users.

• Newly created users are automatically assigned the snc_internal role when they first attempt to log in to the instance, unless they have been explicitly assigned the snc_external role. You can add the snc_external role to a new user before they first log in to the instance to provide external user rights.

**Important:** Activate this plugin during a maintenance window or when few users are logged in. Users currently logged in when the plugin is activated will not be dynamically assigned the snc_internal role. Rather, users must log out and log back in to be assigned the snc_internal role. Once the plugin is activated, you can add or remove the snc_internal and snc_external roles at any time to change user rights.

• All existing ACLs that do not have a role requirement are automatically assigned the snc_internal role. Because both existing ACLs and users are assigned the snc_internal role, existing access levels do not change.
• Newly created ACLs that do not have a role requirement are automatically assigned the snc_internal role. This role assignment does not apply to a newly created ACL with a role assigned.
• For all existing Processor [sys_processor] records or newly created Processor [sys_processor] records with **Type=script**, the snc_internal role is automatically added to the Roles field if the field is empty.
• To restrict access to UI pages to internal users, the plugin automatically assigns the snc_internal role to the * ACL with a **Type of ui_page**.
• To restrict access to processors to internal users, the plugin automatically assigns the snc_internal role to the * ACL with a **Type of processor**.
• External users must obtain, at minimum, the snc_external role to access the instance. This role must be manually granted to external users. Access to records is granted through ACLs.

Do not move system update sets among instances with and without the Explicit Roles plugin enabled. For more information, see System update sets.

**Note:** This plugin also requires the Contextual Security Manager plugin.

**Providing table access to external users**

You can provide external users access to a table by adding a role to the table that inherits the snc_external role. For more information, see Provide external users access to a table.

**The hasRoles() method**

The hasRoles() method is still available, but is deprecated in the Geneva release. Use the hasRole(role name) method instead.

If you do use the hasRoles() method, note these changes:

• This method automatically excludes the default snc_internal role when it checks for roles. This means that if a user has only the snc_internal role, the hasRoles() method still returns false.
• If the user has the snc_external role, the method returns false because the instance considers external users to be without a role.


**Mutual exclusion: snc_external versus snc_internal**

The prevents users from having both the snc_external role and the snc_internal role. The applies this mutual exclusion everywhere in the system and writes error messages to the logs for each conflict.

**Note:** ACLs can have both roles if the ACL resources should be accessible to all users.

Example: Adding both explicit roles to a user (direct collision):

1. Assign user Abel Tuter the snc_internal role.
2. Assign user Abel Tuter the snc_external role.

Result: Adding the snc_external role fails because Abel Tuter has the snc_internal role.

Example: Adding both explicit roles to a group (direct collision):

1. Consider a group called Test Group that currently has no explicit roles assigned to the group.
2. Add Abel Tuter to the Test Group.
3. Add the snc_external role to Test Group.

Result: Adding the snc_external role fails because Abel Tuter already has the snc_internal role and can't have both roles.

Example: Adding an explicit role to a group where a group member has the conflicting explicit role (indirect collision):

1. Assign user Abel Tuter the snc_internal role.
2. Consider a group called Test Group that currently has no explicit roles assigned to the group.
3. Add Abel Tuter to the Test Group.
4. Add the snc_external role to the Test Group.

Result: Adding the snc_external role to the group fails because Abel Tuter would inherit the snc_external role through group membership. Both explicit roles would be assigned to the same user, which isn't allowed.

For other examples, see the following table:

<table>
<thead>
<tr>
<th>Role</th>
<th>Attempted action</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct collision</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The user has the snc_internal role.</td>
<td>Add the snc_external role.</td>
<td>The action is aborted.</td>
</tr>
<tr>
<td>The user has the snc_external role.</td>
<td>Add the snc_internal role.</td>
<td>The action is aborted.</td>
</tr>
<tr>
<td>The user has no explicit role.</td>
<td>Add the snc_internal or snc_external role.</td>
<td>The role is added.</td>
</tr>
<tr>
<td>The user has both explicit roles (existing collision).</td>
<td>Add the user to a group with no roles.</td>
<td>The action is aborted.</td>
</tr>
<tr>
<td>A role not associated with any users contains the snc_internal role.</td>
<td>Add the snc_external role.</td>
<td>The action is aborted.</td>
</tr>
<tr>
<td>A role not associated with any users contains the snc_external role.</td>
<td>Add the snc_internal role.</td>
<td>The action is aborted.</td>
</tr>
<tr>
<td>Role</td>
<td>Attempted action</td>
<td>Result</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>A role contains both explicit roles (existing collision).</td>
<td>Add the role to a user, role, or group.</td>
<td>The action is aborted.</td>
</tr>
<tr>
<td>A group with no members has the snc_internal role.</td>
<td>Add the snc_internal role.</td>
<td>The action is aborted.</td>
</tr>
<tr>
<td>A group with no members has the snc_external role.</td>
<td>Add the snc_internal role.</td>
<td>The action is aborted.</td>
</tr>
<tr>
<td>A group with no members has no roles.</td>
<td>Add the snc_internal or snc_external role.</td>
<td>The role is added.</td>
</tr>
</tbody>
</table>

**Indirect collision**

<table>
<thead>
<tr>
<th>Role containment with collision</th>
<th>1. Grant a role called Test Role to a user with the snc_internal role.</th>
<th>The action is aborted.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role containment without collision</td>
<td>1. Grant a role called Test Role to a user with no roles.</td>
<td>The role is added to both the user and Test Role.</td>
</tr>
<tr>
<td></td>
<td>2. Add the snc_external role to Test Role.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group containment with collision</th>
<th>1. Add a user who has the snc_internal role to a group called Test Group 2 (child of Test Group 1).</th>
<th>The action is aborted.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2. Add the snc_external role to Test Group 2.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Add the snc_external role to a parent group called Test Group 1 (parent of Test Group 2).</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group containment without collision</th>
<th>1. Add a user with no roles to a group called Test Group 2 (child of Test Group 1).</th>
<th>The role is added to the parent group, the child group, and the user.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2. Add the snc_external or snc_internal role to Test Group 1 (parent of Test Group 2).</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group containment plus role containment with collision</th>
<th>Add contains_external to Test Group 1, the parent of Test Group 2.</th>
<th>Test Group 1 and Test Group 2 both get contains_external, but don’t explicitly get the snc_external role.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Add the snc_internal role to Test Group 2, the child of Test Group 1.</td>
<td>The action is aborted.</td>
</tr>
</tbody>
</table>
### Role

<table>
<thead>
<tr>
<th>Attempted action</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Remove Test Group 1 as the parent of Test Group 2.</td>
<td>The action is aborted.</td>
</tr>
<tr>
<td>2. Add the snc_internal role to Test Group 1.</td>
<td>Repeat for already nested groups, with the same expectation.</td>
</tr>
<tr>
<td>3. Add the snc_external role to Test Group 2.</td>
<td></td>
</tr>
<tr>
<td>4. In Test Group 2, set Test Group 1 as the parent group and save.</td>
<td></td>
</tr>
</tbody>
</table>

The cause of an aborted action appears in the error message and must be addressed before another attempt succeeds. For direct cases, such as adding an explicit role to an individual user, verify which explicit role the user should have. If the user has the wrong explicit role, it must first be removed, and then the correct explicit role must be added.

For indirect cases, such as adding an explicit role to a group (so that a group member would be assigned both explicit roles), evaluate whether that user should be in the group. Also determine whether the group should be given the explicit role, including any inheritance through group hierarchy and role containment.

Note that reports only the first potential collision encountered. If repeated attempts continue to fail after remediation, with a new root cause each time, re-evaluate the relevant user/group/role interdependence more broadly. You may want to rethink how groups and role containments are structured.

## Request Explicit Roles

Activate Explicit Roles by requesting the Explicit Roles plugin (com.glide.explicit_roles) through the Now Support Service Catalog.

Role required: admin

**Important:** Activate this plugin during a maintenance window or when few users are logged in. Users currently logged in when the plugin is activated will not be dynamically assigned the snc_internal role. Rather, users must log out and log back in to be assigned the snc_internal role. Once the plugin is activated, you can add or remove the snc_internal and snc_external roles at any time to change user rights.

1. Navigate to System Applications > All Available Applications > All.
2. On the All Applications page, click **Request Plugin** to open the Request form on HI.
3. On Now Support, select the redirect link to access the Now Support Service Portal Service Catalog.

<table>
<thead>
<tr>
<th>Activate Plugin request form</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td>Target Instance</td>
</tr>
<tr>
<td>Plugin Name</td>
</tr>
<tr>
<td>Specify the date and time you would like this plugin to be enabled</td>
</tr>
<tr>
<td>Reason/Comments</td>
</tr>
</tbody>
</table>

4. On the form, fill in the fields.

5. Click Submit.

**Elevated privilege roles**

Elevated privilege roles require you to manually accept the responsibility of using the role before you can access the features of the role.

By default, you do not have elevated privilege roles upon login. You must manually elevate to the privilege of the role. An elevated privilege role lasts only for the duration of your user session. Session timeout or logout removes the role.

You can designate any role as an elevated privilege role, and then assign that role to one or more users. Do this when you want to restrict users from having access to the rights that the role provides immediately after login. You can designate the privilege role on the Role form. See Create a role for instructions.

To use an elevated role, you must meet these conditions:
• The elevated role must be assigned to you.
• You must manually elevate to a specific elevated role to get its privileges, even if you are already elevated to a second elevated role that contains the first elevated role.

For example, if elevated role A contains elevated role B, even if you elevate to role A, you must still elevate to role B to get its privileges.

The admin role

To grant the admin role to a user, the granting user must also have the admin role. For example, a user with only the user_admin role cannot grant the admin role to other users.
• Non-admin users cannot add a user to a group that contains the admin role.
• To grant the security_admin role to a user, the granting user must also have the admin role and must elevate to the security_admin role before granting the security_admin role to other users. A user with only the admin role cannot grant the security_admin role to other users.
• A user without the security_admin role cannot add a user to a group that contains the security_admin role.

Warning: The use of elevated privilege on the admin role is not supported and may cause unexpected behavior. To require administrators to manually elevate, see Force administrators to manually elevate.

The security_admin role

In the base system, the security_admin role is the only role that has elevated privileges. This role is automatically assigned to the user who is the default System Administrator (admin) user. It provides access to ACLs and High Security Settings.
Roles assigned to the System Administrator (admin) user

Note: To see this role, you must actually elevate to the security_admin role first. If you are logged in as the System Administrator (admin) user only, you cannot see the security_admin record in the list of roles.
The security_admin role record

security_admin role

The security_admin role is an elevated privilege role provided with High Security Settings that lets users create and change access controls and change High Security Settings.

In the base system, only the default System Administrator (admin) user has the security_admin role. Since it requires elevating privileges, the admin user does not have this role at login. After elevating privileges, the admin user has the security_admin role for the duration of the user session.
**Note:** The record for the System Administrator (admin) role is only visible to users who elevate privileges to the security_admin role.

To maintain high security, the security_admin role requires elevating privileges. Limit the users and groups to which you assign this role.

**Elevate to a privileged role**

The base system admin can elevate to a privileged role to have access to the features of High Security Settings.

Role required: admin

**Note:** If you grant additional users the admin role, they cannot elevate to a privileged role. Only the out-of-box admin can elevate.

1. Do the appropriate action for your version of the UI:

| UI16 |  
|------|---
| a.   | In the banner frame, click your user name.  
| b.   | Select **Elevate Roles**. |
In the banner frame, click the lock icon (🔒) by your user name.

A dialog box appears.

2. Select an elevated role and click OK. This role grants the user elevated privileges to all resources controlled by the role for the remainder of the session. When the user logs out, the elevated privileges are terminated and must be reestablished at the next login. When elevated privileges are activated, the icon has an unlocked appearance.

Note: Any edits being made when the page reloads are lost.

**Force administrators to manually elevate**

A property is available to force all users with the administrator role to manually select the role they want to elevate to.

Role required: security_admin

1. Log in as admin.
2. Elevate your role to security_admin.
3. Navigate to sys_properties.list.
4. Search for and select the glide.security.strict_elevate_privilege property.
5. Set the Value field to true and click Submit.

When the user logs in, they are presented with a dialog window to select the role to which they can elevate.
Login and authentication security

Configure login security options to control access to your instance.

Security options

You can control several aspects of user login and authentication security:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Related topics</th>
</tr>
</thead>
</table>
| Log in and log out controls | Control several dimensions of the log in and log out process for users, such as specifying a landing page that the user sees upon login and control how users log out. | • Define login scenarios  
• Enable the logout confirmation prompt  
• Remove the Logout button  
• Installation exits  
• Specify lockout for failed login attempts |
| Authentication security | Control the password reset process and features like the Remember Me option. You can also use IP address-based controls for access to the instance and implement a nonce to be used with single sign-on digest authentication. | • Strengthen password validation rules  
• Example: The default self-service Password Reset process  
• Change settings for the Remember me check box and cookie  
• IP range based authentication  
• Implementing a nonce |
Define login scenarios

You can direct all users to the same page after login.

Role required: admin

When users log on to an instance directly, such as going to http://[instance_name].service-now.com/, the system does the following:

1. Accesses the value in the property `glide.entry.page.script`. The default value of the property is derived from a script include named `CMSEntryPage`.
2. Directs the user to the instance login page if the entry page requires a login.
3. Applies login rules, if any, to the user.

To force the system to direct all users to the same page after login:

1. Navigate to `Content Management > Configuration > Configuration Page`.
2. Select a value for the `Login page` field, or create a new page as desired. If this page is not the site default page, it always redirects here. If it is a site default page, it applies login rules. If this value is null, the system uses `navpage.do` as the entry page. Do not enter a login page here; otherwise, users need to log in twice.

Logging Into an Instance to access a record:

When users log into an instance to access a record by its globally unique identifier (sys_id), such as http://[instance].service-now.com/incident.do?sys_id={sys_id}, then the system does the following:

a. Directs the user to a login page if not already logged in.

b. Directs the user to the appropriate record if they are allowed to access it. If the user does not have access rights to the record, a denial of access message appears.

Logging Into the Service Portal or a CMS site:

When users log on the Service Portal or a CMS site, such as http://<instance>.service-now.com/site-name/page.do, the system does the following:

- If there is a value in the `Login page` field on the Service Portal or the CMS site form, it directs the user to that login page and applies login rules, if any, to the user.
- If there is no login page specified, it directs the user to the value in the `Home page` field on the Service Portal or the CMS site form.

Logging Into the Service Portal or a CMS Site to access a record:

When users log on to the Service Portal or a CMS site to access a record, such as http://{instance}.service-now.com/ess/incident_detail.do?sysparm_document_key=incident,{sys_id}, the system follows the same procedure and finally takes the user to the record. If the user does not have access rights to the record, a denial of access message appears.

Logins and the employee self-service portal

The system keeps track of the first starting page that a user is trying to access even if the user wants to log in to the Employee Self-Service Portal.

Consider the following scenarios.

Example 1:

1. A user is not logged in, and then tries to access a record using a specific SYS ID in the URL.
2. The system redirects the user to the login page.
3. Rather than logging in, the user tries to access another site, such as the Employee Self-Service (/ess) Portal.
4. The system redirects the user to the login page again.
5. The user logs in and is redirected to the record that the user was first trying to access rather than the Employee Self-Service Portal.

Example 2:
1. A user is not logged in, and then tries to access a record using a specific SYS ID in the URL through the Employee Self-Service (/ess) Portal.
2. The system redirects the user to the login page.
3. Rather than logging in, the user tries to access another record through the Employee Self-Service Portal.
4. The system redirects the user to the login page again.
5. The user logs in and is redirected to the first record rather than the second.

Specify a login landing page

By default, users see their homepage upon login. You can specify a different login landing page by using a system property or the content management system.

Role required: admin

To specify a login landing page for all users, change the property value on the sys_properties table.

1. Type sys_properties.list in the navigation filter.
2. Locate the glide.login.home system property.
3. In the Value field, enter the name of the page that all users see upon login.

Use <page name>.do; you may omit the http://''instance''.service-now.com/ portion of the URL. To determine the page name or the URL of a page in the system, you can point to a link. Some possible pages are welcome.do and incident.do.

To specify a dashboard landing page, set the property to $dashboards.do?dashboard=<SYS_ID>. Replace <SYS_ID> with the sys_id of the dashboard.

Note: This property is system-wide, so setting it affects all users.

You can also specify a login landing page with the content management system.

Specify lockout for failed login attempts

The system provides inactive script actions that enable you to specify the number of failed login attempts before a user account is locked and to reset the count after a successful login.

Role required: admin

Navigate to System Policy > Script Actions to view or activate the scripts.

Note: Starting with the Kingston release, following a zBoot, the script actions SNC User Lockout Check with Auto Unlock and SNC User Clear are activated.
To learn more about properties that affect failed login attempts, see Managing failed login attempts (instance security hardening) in the Instance Security Hardening Settings.

<table>
<thead>
<tr>
<th>Script action</th>
<th>Description</th>
</tr>
</thead>
</table>
| SNC User Lockout Check with Auto Unlock | • Uses the value of the glide.user.max_unlock_attempts property to set the limit for failed login attempts.  
• Unlocks the user account after the time period that is specified for the glide.user.unlock_timeout_in_mins property. If no value is specified, then the system unlocks the user account after the default period of 15 minutes. |
| SNC User Lockout Check | Tracks the number of failed login attempts and locks the user account after a specified number of failed login attempts (default: 5). |
| SNC User Clear | Updates the user record after a successful login: Resets the number of failed login attempts and updates the date of the last login. |

Each time a user attempts to log in, the action is recorded in an event log. You can view a log of failed login attempts.

1. Navigate to System Policy > Event Logs.
2. Filter for login.failed in the Name field. You can view the attempted login name, date, and IP address logged for the attempt.

Make UI pages public or private

You can make pages public if you want your users to see the pages without logging in.

Role required: admin

Most pages are only viewable by logged in users. A limited number of pages are public so that users do not have to log in to view them, such as the welcome page, the front page, and the login and logout pages.

⚠️ Warning: Several base system public pages are required for the functionality of many features. Do not disable base system public pages.

1. In the application navigator filter, type sys_public.list.
2. Click New.
3. In the sys_public table, create a record with the following values.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Page</td>
<td>The name of the page. For example: $sp</td>
</tr>
<tr>
<td>Active</td>
<td>When selected, the page is publicly accessible. Deselect the Active option when you want the page to be private.</td>
</tr>
</tbody>
</table>

4. Click Save.

By setting active to true, the page is public, so anyone visiting <instance_name>/sp or <instance_name>/sp.do can access the page.

Enable the logout confirmation prompt

You can enable a logout confirmation prompt to prevent users from inadvertently logging themselves out.
Role required: admin

Note: The following procedure only works in UI versions earlier than UI16, which is the most recent and most commonly used one.

1. Navigate to System Properties > System.
2. Locate the Prompt user to confirm a logout request property and select the check box.
3. When the user clicks the Logout button, a confirmation dialog box displays.

![Confirmation dialog box](example.png)

Remove the Logout button

You can remove the Logout button to prevent inadvertent logouts.

Role required: admin

Note: The following procedure does not work in UI16.

1. Navigate to User Administration > User Preferences.
2. Delete the system preference user.can.logout.

Installation exits

Installation exits are customizations that exit from Java to call a script before returning back to Java.

Note: Functionality described here requires the Admin role.

Available installation exits

Navigate to System Definition > Installation Exits. Some installation exit names (Login, Logout, ValidatePassword, ExternalAuthentication) are reserved and cannot be changed. Other installation exits can override these with custom script that replaces the script in the default installation exit.

The following installation exits are available in the base system:

<table>
<thead>
<tr>
<th>Installation Exit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login</td>
<td>Takes a username and password pair and authenticates with the user object</td>
</tr>
<tr>
<td>Logout</td>
<td>Takes the user to the welcome page upon signing out; can be overridden by LogoutRedirect</td>
</tr>
</tbody>
</table>
### Installation Exit

<table>
<thead>
<tr>
<th>Installation Exit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LogoutRedirect</td>
<td>Takes the user to a specified URL upon signing out</td>
</tr>
<tr>
<td>ExternalAuthentication</td>
<td>Authenticates using header, parameter, or cookie; can be overridden by DigestSingleSignOn and PGPSingleSignOn</td>
</tr>
<tr>
<td>DigestSingleSignOn</td>
<td>Authenticates using header, parameter, or cookie and decrypts Digest encryption</td>
</tr>
<tr>
<td>PGPSingleSignOn</td>
<td>Authenticates using header, parameter, or cookie and decrypts PGP encryption</td>
</tr>
<tr>
<td>ValidatePassword</td>
<td>Active by default, starting with the Helsinki release; allows customers to define their own password validation; can be overridden by ValidatePasswordStronger</td>
</tr>
<tr>
<td>ValidatePasswordStronger</td>
<td>Requires passwords be at least 8 characters long and contain a digit, an uppercase letter, and a lowercase letter</td>
</tr>
<tr>
<td>GetIntegrationSessionTimeout</td>
<td>Implements the default integration session timeout behavior.</td>
</tr>
</tbody>
</table>

### Login modifications

The following modification to the `Login` installation exit sets each user's session timeout value as the user is logging in. In this particular example, if the user name is `admin`, the session is set to timeout in 30 seconds.

```javascript
gs.include("PrototypeServer");

var Login = Class.create();
Login.prototype = {
  initialize : function() {
  },

  process : function() {
    // the request is passed in as a global
    var userName = request.getParameter("user_name");
    var userPassword = request.getParameter("user_password");

    var authed = GlideUser.authenticate(userName, userPassword);
    if (authed) {
      // ***********************************************************
      // customization - if the userName == admin, set the session
      // timeout to be 30 seconds. You can implement your own
      // session timeout algorithm here by checking to see if a user
      // belongs to a certain group or has a certain role.
      // Values of setTimeout exceeding 1440 minutes are
      // treated as one day (1440 minutes).

      if (userName == "admin") {
        request.getSession().setMaxInactiveInterval(30);
      }
      // ***********************************************************
      return GlideUser.getUser(userName);
    }

    this.loginFailed();
  }
};
```
return "login.failed";
},

loginFailed : function() {
    var message = GlideSysMessage.format("login_invalid");
    var gSession = GlideSession.get();
    gSession.addErrorMessage(message);

    var userName = request.getParameter("user_name");
    EventManager.queue("login.failed", ",", userName, ",");
}
}

Session timeout can also be set according to IP address.

gs.include("PrototypeServer");

var Login = Class.create();
Login.prototype = {
    initialize : function() {
    },

    process : function() {
        // the request is passed in as a global
        var userName = request.getParameter("user_name");
        var userPassword = request.getParameter("user_password");

        var authed = GlideUser.authenticate(userName, userPassword);
        if (authed) {
            // **************************************************************
            // customization - if the user is logging in from a particular IP
            // range starting with XXX.XXX you can implement your own
            // session timeout algorithm here by checking the login IP
            // / *
            // Values of setMaxInactiveInterval exceeding 1440 minutes are
            // treated as one day (1440 minutes).
            var clientIP = gs.getSession().getClientIP().toString();
            if (clientIP.indexOf('XXX.XXX') == 0) {
                // set to 10 hours
                request.getSession().setMaxInactiveInterval(60 * 60 * 10);
            }
            // **************************************************************
            return GlideUser.getUser(userName);
        }

        this.loginFailed();
        return "login.failed";
    },

    loginFailed : function() {
        var message = GlideSysMessage.format("login_invalid");
        var gSession = GlideSession.get();
        gSession.addErrorMessage(message);

        var userName = request.getParameter("user_name");
        EventManager.queue("login.failed", ",", userName, ",");
    }
}
Strengthen password validation rules

You can customize password strength validation rules for the change password screen by overriding the installation exit associated with password validation.

1. Navigate to System Definition > Installation Exits.
2. Locate ValidatePassword (inactive by default) and ValidatePasswordStronger (active by default, starting with the Helsinki release).
3. The ValidatePasswordStronger script (below) is a sample script that overrides the ValidatePassword script by using regular expressions to require that passwords be a minimum of 8 characters long, contain a numeric digit, and contain mixed-case letters.

```javascript
gs.include("PrototypeServer");
var ValidatePasswordStronger = Class.create();
ValidatePasswordStronger.prototype = {
  process : function() {
    var user_password = request.getParameter("user_password");
    var min_len = 8;
    var rules = "Password must be at least " + min_len + " characters long and contain a digit, an uppercase letter, and a lowercase letter."
    if (user_password.length() < min_len) {
      gs.addErrorMessage("TOO SHORT: " + rules);
      return false;
    }
    var digit_pattern = new RegExp("[0-9]", "g");
    if (!digit_pattern.test(user_password)) {
      gs.addErrorMessage("DIGIT MISSING: " + rules);
      return false;
    }
    var upper_pattern = new RegExp("[A-Z]", "g");
    if (!upper_pattern.test(user_password)) {
      gs.addErrorMessage("UPPERCASE MISSING: " + rules);
      return false;
    }
    var lower_pattern = new RegExp("[a-z]", "g");
    if (!lower_pattern.test(user_password)) {
      gs.addErrorMessage("LOWERCASE MISSING: " + rules);
      return false;
    }
    return true; // password is OK
  }
}
```

The script variable created by Class.create() must have the same name as the installation exit itself—"ValidatePasswordStronger" in this example. The script implements the process() function which returns true if the password is acceptable and false if the password must be revised. The gs.addErrorMessage function can be used to return error messages on the change password screen. You can try this Installation Exit in your instance by checking the active flag and updating the record. Be sure and clear the cache after doing this so the change is recognized.

Also, keep in mind that modifying these scripts will not change the default ServiceNow behavior: Blank passwords are still prohibited by default and the password and verify password fields must match.
To test, check the **Password needs reset** box on a user record then login with that user. Validation will occur at the point that the user attempts to set the password. Validation does not apply when an admin user updates the password in the user record directly (the admin can put anything in the password field).

**Note:** The change password screen only applies to customers who do not use single sign on and are not integrated with their local LDAP.

**Example: The default self-service Password Reset process**

The default self-service Password Reset process enables a user to reset the password without assistance from service desk agents.

**The default self-service password reset flow**

1. If a user does not remember the password, the user can click the **Forgot Password?** link on the login screen.

2. The Password Reset application starts. On the **Identity** page, the user identifies himself or herself by entering a **Username**.

3. On the **Verify** page, the user proves that they are the person who is associated with the username. In this example, the user enters the email address that is associated with the user profile. The admin can configure a different verification method or can require additional verifications, for example, a personal question that only the user can answer.
4. The Reset page tells the user to check email for instructions.

5. The user opens the email and clicks the here link to reset the password. The link is valid for a period that you specify (use the `password_reset.request.expiry` property).

6. The Reset Password page guides the user to reset the password.

The default self-service Password Reset process (`com.glideapp.password_reset`) defines:

- The URI that specifies where users are redirected when they click Forgot Password?. By default this value is `/Spwd_reset.do?sysparm_url=ss_default`, which is the same value used in the `glide.security.password_reset.uri` property. In previous releases, this value was set to `/reset_password.do`.
- The Enable Password Reset URL option, which specifies that the user should receive an email with a link to reset their password after they click Forgot Password?.
- The Personal Data - Enter Email Address verification flow that specifies the three-step password reset flow.

See for instructions on accessing this form and configuring the fields.
Modify the Password Reset notification email text

Users of the self-service Password Reset process receive an email notification when they request password reset. You can modify the text of the email and other aspects of the notification.

Role required: admin

This process is relevant only if users are subscribed to the notification.

1. Navigate to System Notification > Notifications.
2. Select the Password Reset URL notification.
3. Modify the text of the email in the What it will contain section.

For information on configuring other aspects of the notification, see Create an email notification.

Configure Password Reset properties

You can specify properties that configure the Password Reset experience for end users.

Role required: password_reset_admin

While there are no range limits for the values you can enter for properties, consider using only positive integer values starting at 1. When you determine the limit for the upper range of a property, consider the task that the user is performing.

For example, you would not want to allow 100 attempts for users to verify their identity. A more common value is 3 attempts. Similarly, you may not want to force users who are completing the enrollment process to spend time selecting and answering 30 security questions. The more commonly used number of security questions is between 5 and 7.

1. Navigate to Password Reset > Properties.
2. Update settings as needed and then click Save.

<table>
<thead>
<tr>
<th>Property Label</th>
<th>Property Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Reset Global properties</td>
<td>password_reset.enrollment_reminder.email_template</td>
<td>Template to use for the email messages that remind users to enroll for the password reset process. See Send email to remind users to enroll for Password Reset.</td>
</tr>
<tr>
<td>Property Label</td>
<td>Property Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Workflow polling frequency</td>
<td>password_reset.wf.refresh_rate</td>
<td>Time period in milliseconds between checks on status of the Password Reset workflow.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: 500</td>
</tr>
<tr>
<td>Workflow expiration</td>
<td>password_reset.wf.timeout</td>
<td>Maximum wait time in milliseconds for the workflow to complete. The workflow is triggered during the password reset request when the user clicks Submit.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: 90000</td>
</tr>
<tr>
<td>Disable CAPTCHA validation functionality</td>
<td>password_reset.captcha.ignore</td>
<td>Enables or disables CAPTCHA functionality.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: false</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The Password Reset application uses Google re-CAPTCHA as the default CAPTCHA service. To use the base system CAPTCHA, change the password_reset.captcha.google.enabled system property to false. See Configure Google reCAPTCHA</td>
</tr>
<tr>
<td>Password Reset Request properties</td>
<td></td>
<td>Number of unsuccessful attempts allowed to reset/change password</td>
</tr>
<tr>
<td></td>
<td>password_reset.request.max_attempt</td>
<td>Number of password reset attempts a user is allowed before they are locked out for a period determined by the value in max_attempt_window.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: 3 (attempts)</td>
</tr>
<tr>
<td></td>
<td>password_reset.request.max_attempt_window</td>
<td>Time period that users are blocked or prevented from changing their passwords after trying the maximum number of times.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: 1440 (minutes)</td>
</tr>
<tr>
<td>Property Label</td>
<td>Property Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------</td>
<td>----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Number of minutes a user must wait to reset/change password after the last</td>
<td>password_reset.request.success_window</td>
<td>Time period that a user must wait after successfully resetting the password to reset the password again.</td>
</tr>
<tr>
<td>successful reset/change</td>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: 1440 (minutes)</td>
</tr>
<tr>
<td>Number of minutes a user must wait to start a reset request after the last</td>
<td>password_reset.request.unlock_window</td>
<td>Time period that a user must wait after a successful unlock operation before starting a new request.</td>
</tr>
<tr>
<td>successful unlock account</td>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: 1440 (minutes)</td>
</tr>
<tr>
<td>Number of minutes before a password reset request expires</td>
<td>password_reset.request.expiry</td>
<td>Time period during which a user must perform the Password Reset process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: 10 (minutes)</td>
</tr>
</tbody>
</table>

**Note:** This setting takes precedence over the `glide.pwd_reset.onetime.token.validity` property (that has a 12-hour default).

### Password Reset Security Question properties

<table>
<thead>
<tr>
<th>Minimum number of characters in any answer</th>
<th>password_reset.qa.ans_min_len</th>
<th>Minimum number of alphanumeric characters that the user must enter in the answer text box for any security question.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Default value: 3 characters</td>
</tr>
<tr>
<td>Property Label</td>
<td>Property Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------</td>
<td>----------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Number of security questions required during the password reset request</td>
<td>password_reset.qa.num_reset</td>
<td>Number of security questions that are displayed on the Verify page while a user is attempting to reset the password. The user must answer all questions correctly to verify identity. The questions are selected at random and are presented in random order.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: 3 (questions)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Possible values: Integers that are less than the number specified for the <strong>Number of security questions required during enrollment</strong> property (the <code>num_enroll</code> parameter).</td>
</tr>
<tr>
<td><strong>Note:</strong> You can override this property setting for a Password Reset process by configuring the <code>num_reset</code> parameter. See Specify the number of required security questions.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Property Label</td>
<td>Property Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Number of security questions required during enrollment | password_reset.qa.num_enroll | Number of questions that a user must provide answers to while enrolling for the Password Reset process.  
- Type: integer  
- Default value: 5  
- Possible values: Integers that are greater than or equal to the number specified for the **Number of security questions required during enrollment** property (the num_reset parameter). |

**Note:** While attempting to verify identity, if a user answers a question incorrectly, the application refreshes with a random set of the specified questions in random order. You should, therefore, require more questions than specified for the **Number of security questions required during enrollment** property (the num_reset parameter).  
**Note:** You can override this property setting for a Password Reset process by configuring the num_enroll parameter. See Specify the number of required security questions.
<table>
<thead>
<tr>
<th>Property Label</th>
<th>Property Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Maximum number of SMS codes sent for verification per day | password_reset.sms.max_per_day               | Maximum number of SMS codes that are sent to a user within one 24-hour period. The 24-hour period begins when a user clicks **Send Code**.  
• Type: integer  
• Default value: 10 (per day)  

**Note:** You can override this SMS code property by adding the **max_per_day** parameter in the SMS code verification. |
| Number of minutes before the user can attempt to send another SMS code for verification | password_reset.sms.pause_window               | Time that must pass before another SMS code can be sent to a user.  
• Type: integer  
• Default value: 2 (minutes)  

**Note:** You can override this SMS code property by adding the **pause_window** parameter in the SMS code verification. |
| Number of digits in the SMS code sent to the user | password_reset.sms.default_complexity        | Number of characters required for a user to reset their password.  
• Type: integer  
• Default value: 4 (digits)  

You can override this SMS code property by adding the **complexity** parameter in the SMS code verification. |
<table>
<thead>
<tr>
<th>Property Label</th>
<th>Property Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of minutes before the SMS code expires</td>
<td>password_reset.sms.expiry</td>
<td>Time, in minutes, until the SMS code sent to the user expires.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: 5 (minutes)</td>
</tr>
<tr>
<td>Note: You can override this SMS code property by the expiry parameter in the SMS code verification.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password Reset Monitoring and Reporting properties</td>
<td>password_reset.activity_monitor.incident_window</td>
<td>Time window to count the number of blocked users.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: 60 (minutes)</td>
</tr>
<tr>
<td>Number of blocked users, in the defined time interval, that triggers a system log event</td>
<td>password_reset.activity_monitor.incident_threshold</td>
<td>Number of blocked (or locked) users, within the specified time window, that triggers a system log event.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: 10 (blocked users)</td>
</tr>
<tr>
<td>Password Reset Style Sheet</td>
<td>password_reset.stylesheet</td>
<td>Name of a custom CSS style sheet in the Style Sheet [content_css] table. You can use the default style sheet as a template for the custom style sheet. You cannot add element definitions to the style sheet.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: css_pwd_reset_default</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Property Label</th>
<th>Property Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email template for reminder emails</td>
<td>password_reset.email_template_default</td>
<td>Template to use to specify the subject and body of the email messages to remind users to enroll for the Password Reset process. For example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• [Subject] Reminder: Enroll in the Password Reset program</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• [Body] Click here to enroll for the password reset service.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> You must create an email template in the password_reset table to use it as a reminder.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: email_template_default</td>
</tr>
</tbody>
</table>

**Note:** Several components in the Self Service Password Reset (com.snc.password_reset) plugin and the Password Reset (com.glideapp.password_reset) plugin control the password reset flow. The following properties affect Password Reset, but do not appear on the Password Reset Properties page:

- You can add the glide.pwd_reset.onetime.token.validity property to the System Properties [sys_properties] table to specify the number of hours that the Password Reset token should be valid. Default: 12.

**Note:** The setting for the password_reset.request.expiry property (time period during which a user must perform the Password Reset process) takes precedence over the setting for glide.pwd_reset.onetime.token.validity.

Properties accessible from the System Properties [sys_properties] table:

- For Password Reset on mobile devices, you can specify the URL that the user is taken to when user taps the Forgot password? button. See the glide.security.password_reset.uri property in High Security Settings. Default: /pwd_reset.do?sysparm_url=ss_default
- If glide.security.forgot_password.display.link is set to true, displays the Forgot Password? link on the login page.
Change settings for the Remember me check box and cookie

When the Remember me check box is selected at login, a cookie is stored on the user's computer. This cookie automatically authenticates the user upon subsequent visits.

If the user logs out, the cookie is destroyed. The default value of the Remember me check box is controlled by one property, and whether or not the check box appears on the login page is controlled by a different property.

Two properties, glide.ui.user_cookie.life_span_in_days and glide.ui.user_cookie.max_life_span_in_days control the glide_user system generated cookie expiration value. When a user accesses an instance with 'remember me' enabled, the access resets the cookie expiration period until the maximum (glide.ui.user_cookie.max_life_span_in_days) life span limit is reached.

Note: To learn more about these properties, see the following topics in Instance Security Hardening Settings:
• Absolute session timeout (instance security hardening)
• Session window timeout (instance security hardening)

Change the default value of the Remember me check box

You can change the default value of the Remember me check box.

Role required: admin

1. Navigate to System Properties > UI Properties.
2. Locate the Default value of "Remember me" checkbox on login page property (glide.ui.remember.me.default).
3. To set the default value of the Remember me check box to No, clear the property check box.
4. To restore the default value of the Remember me check box to Yes, select the property check box.

Remove the Remember me check box

You can remove the Remember me check box so users do not have access to this feature.

Role required: security_admin

Note: To learn more about this property, see Remove remember me (instance security hardening) in Instance Security Hardening Settings.

1. Elevate your role to security_admin.
3. Locate the Remove "Remember me" checkbox from login page property (glide.ui.forgetme).
4. Select the property check box.
   This setting removes the Remember me check box, invalidates existing cookies, and disables Remember me functionality entirely.
5. To restore the Remember me check box to the login page, clear the property check box.

IP range based authentication

One way to secure a web-based application is to restrict access based on the IP address.

You can block access to a specific address or range of addresses that you suspect belong to malicious individuals. The instance allows you to control access by IP address.
Notes and Limitations:

- The system won't let you lock yourself out, so if you try to add a rule such that your current address would be locked out, the system warns you and refuses your insert.
- If you're inside of a corporate intranet, be very careful about setting up your IP rules. The IP address you see on your own computer (like 10.10.10.25) generally bears no relationship to the IP address you'll actually appear as out on the internet. Your company likely proxies and/or NATs your address into a predictable set of outbound addresses which you'll likely need to ask your network team about.
- A user whose access is restricted based on an access rule gets a 403 error on their browser.
- Restricted users do not use transactions, semaphores, or count towards any server resource counts.
- This feature does not supersede or override your existing access control rules if, for example, you're running a VPN to our data center. It's an additional check that must be met in addition to any access controls we may have set up on your PIX.
- Allow rules always supersede deny rules. So if an address is both allowed (by one rule) and denied (by a second rule) it is, in fact, allowed.
- Asterisks and CIDR blocks are not currently supported.
- Regarding forwarded proxy addresses, the allow rules are applied to each address in the chain and then the deny rules are applied to each address in the chain if none of the allow rules matched.

**Note:** To learn more about the com.snc.ipauthenticator and glide.ip.authenticate.strict properties, which restrict instance access to specific IP ranges, see the following topics in Instance Security Hardening Settings:
- Restrict access to specific IP ranges (instance security hardening)
- Strict IP restriction (instance security hardening)

### IP Address Access Control

Apply an IP access control to outbound traffic, inbound traffic, or bidirectional traffic. The system only blocks an IP address if a matching Deny rule exists and no matching Allow rule exists. By default, there are no restrictions on access to your instance.

**Role required: admin**

1. Navigate to **System Security > IP Address Access Control** to see a list of your IP access controls. You might have to activate the IP Range Based Authentication [com.snc.ipauthenticator] plugin.
2. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of access control rule to include.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Allow</strong>: Any IP address in this range can interact with this instance.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Deny</strong>: Any IP address in this range cannot interact with this instance unless it is listed in an Allow rule. Also, when adding deny rules, you cannot deny your own public IP address or your instance does not update a deny rule.</td>
</tr>
</tbody>
</table>

**Note:** To support maintenance, upgrades, and Customer Service and Support, some ServiceNow internal IPs cannot be blocked by Deny rules.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direction</td>
<td>The direction of the IP access control rule.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Inbound</strong>: Allows or denies inbound transactions.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Outbound</strong>: Allows or denies outbound transactions.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Bidirectional</strong>: Allows or denies both inbound and outbound transactions.</td>
</tr>
</tbody>
</table>
## Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>When selected, the form is active.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the access control.</td>
</tr>
<tr>
<td>Range Start</td>
<td>The starting range of IP addresses to allow or deny.</td>
</tr>
<tr>
<td>Range End</td>
<td>The ending range of IP addresses to allow or deny.</td>
</tr>
</tbody>
</table>

**Note:** These rules also affect transferring update sets. To ensure that IP address access control does not cause update sets to fail, add the target instance as an exception.

**Note:** To limit access to specific VPN addresses only, enter a Deny range of 0.0.0.0 through 255.255.255.255 into the Deny field, and only enter the specific allowed VPN ranges.

3. Click **Submit**.

### Find denied IP addresses

Denied IP addresses are by default not viewable from the system logs. However, you can still find them in the instance's node log files.

**Role required:** admin

Log entries for blocked IP address appear as follows:

```
```

1. Navigate to **System Logs > Utilities > Node Log File Browser**.
2. Browse the logs by criteria, such as time period and message.
3. You can also download log files when you know which log you are looking for, by navigating to **System Logs > Utilities > Node Log File Download**.

### Implementing a nonce

You can implement a nonce to be used with single sign-on digest authentication.

To use a nonce with the unencrypted token or encrypted token methods of single sign on, these steps apply with only a few minor changes.

**Note:** The nonce is used only for login requests, not for any other type of request. If the system receives a nonce value after login, the nonce is not consumed.

### Benefits

The usage of a nonce prohibits a malicious user from performing a replay attack in order to log into your system.

### Nonce process flow

When a customer has implemented the digested token Single Sign-on and wishes to add the security of a nonce, they follow a certain process flow.
1. A user logs into the customer's portal.

2. The customer generates the required SSO parameters and appends a random nonce to the end. For example, if the customer were forwarding the authentication response via the query string, it may look something like this:

   SM_USER=itil&DE_USER=V1QuWMnxSfBgfRS099XOcAjKo5Q=&NONCE=1407743018

The instance receives this request and retrieves the authentication variables. Before attempting to verify the integrity of the authentication response, the instance checks the nonce against an internal table (u_authentication_nonce) to verify that it does not yet exist. If the nonce does not exist within that table, the nonce is then added to the table and the authentication process is allowed to continue. However, if that nonce value already exists within the table, the authentication attempt is cancelled and an error code of failed_missing_requirement is returned, which typically takes the user back to the login page.

**Implement a nonce**

Add a cryptographic nonce to the authentication header to ensure that it can only be used once.

- Create a system property called glide.authenticate.header.nonce_key and set its value to whatever variable name you're using for the nonce, such as NONCE or NCE.
- Create a new table called u_authentication_nonce. Add a field to the table called u_nonce.
- Go to System Properties > Installation Exits and create an item called DigestSingleSignOnNonce which overrides ExternalAuthentication (see image below).

![Installation Exit](image)

- Add the following code to the script portion of the newly created DigestSingleSignOnNonce.

```javascript
gs.include("PrototypeServer");
var DigestSingleSignOnNonce = Class.create();
DigestSingleSignOnNonce.prototype = {
    process : function() {
        var headerKey = GlideProperties.get("glide.authenticate.header.key", "SM_USER");
        var headerDigestKey = GlideProperties.get("glide.authenticate.header.encrypted_key", "DIGEST");
        var headerNonceKey = GlideProperties.get("glide.authenticate.header.nonce_key", "NCE");
```
var fieldName = GlideProperties.get("glide.authenticate.header.value", "user_name");
var fkey = GlideProperties.get("glide.authenticate.secret_key");

// Look in the Headers
var data = request.getHeader(headerKey);
var encdata = request.getHeader(headerDigestKey);
var nonce = request.getHeader(headerNonceKey);

// If not, then check the URL Parameters
if (data == null || encdata == null || nonce == null) {
  data = request.getParameter(headerKey);
  encdata = request.getParameter(headerDigestKey);
  nonce = request.getParameter(headerNonceKey);
}

// then maybe its a cookie
if (data == null || encdata == null || nonce == null) {
  var cookies = request.getCookies();
  data = GlideCookieMan.getCookieValue(cookies, headerKey);
  encdata = GlideCookieMan.getCookieValue(cookies, headerDigestKey);
  nonce = GlideCookieMan.getCookieValue(cookies, headerNonceKey);
}

// if found run encryption
if (data != null && encdata != null && nonce != null) {
  try {
    // Replace all spaces with plus(+)’s, converted in url
    encdata = encdata.replaceAll(' ', '+');

    // ----- Encrypt the username|nonce
    var key = this.getDigest(data + "|" + nonce, fkey);

    // Check for match of received encoded data
    // and your encoding of user name
    if (encdata == key) {
      var ugr = new GlideRecord("sys_user");
      ugr.initialize();
      if (!ugr.isValidField(fieldName)) {
        GlideLog.warn("External authorization is set to use field: "+
        fieldName + " which doesn't exist");
        return "failed_missing_requirement";
      }
      ugr.addQuery(fieldName, data);
      ugr.query();
      if (!ugr.next()) { return "failed_authentication";
        ugr.initialize();
        ugr.addQuery(fieldName, data);
        ugr.query();
        if (!ugr.next())
          return "failed_authentication";
      }
      if (this.processNonce(nonce)) {
        var userName = ugr.getValue("user_name");
        return userName;
      } else return "failed_missing_requirement";
  
  } else return "failed_missing_requirement";
}
} else {
    return "failed_authentication";
}
} catch(e) {
    gs.log(e);
    return "failed_authentication";
} // Encoded data didn't match received encoded data
} else {
    return "failed_missing_requirement";
}
,

getDigest : function( data, fkey ) {
    try {
        // default to something JDK 1.4 has
        var MAC_ALG = "HmacSHA1";
        return SncAuthentication.encode(data, fkey, MAC_ALG);
    } catch (e) {
        gs.log(e.toString());
        throw 'failed_missing_requirement';
    }
},

processNonce : function( sentNonce ) {
    var ngr = new GlideRecord("u_authentication_nonce");
    ngr.addQuery("u_nonce", sentNonce);
    ngr.query();
    if (ngr.next()) {
        gs.log("This SSO entry has already been processed! (Nonce: " + sentNonce + ")");
        return false;
    }
    var ngrNew = new GlideRecord("u_authentication_nonce");
    ngrNew.initialize();
    ngrNew.u_nonce = sentNonce;
    ngrNew.insert();
    gs.log("Inserted new nonce: " + sentNonce);
    return true;
}

- Once you've saved your new installation exit, go to the DigestSingleSignOn installation exit and make sure that it is set Active=false.

Your instance should now be configured to implement a nonce.

Certificates

Your instance requires certificates to establish secure connections and validate signatures.

Certificates are used for features such as:

- LDAPS
- Outbound web services mutual authentication
- Web services security
• MID Server

In order to use a certificate, you need to generate or purchase a certificate for the secured server or client and upload it to an instance.

LDAP certificates

An SSL certificate is required for the instance to establish an LDAP over SSL (LDAPS protocol) connection with an LDAP server.

The instance accepts two types of LDAP certificates:

<table>
<thead>
<tr>
<th>Certificate</th>
<th>Type</th>
<th>Required for</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP server certificate</td>
<td>Any supported type</td>
<td>All LDAP configurations</td>
</tr>
<tr>
<td>LDAP client certificate</td>
<td>Java keystore type</td>
<td>Mutual authentication</td>
</tr>
</tbody>
</table>

If there are multiple server certificates, the instance tries each server certificate in turn until the LDAP server allows the connection. If you use multiple LDAP servers, be sure to include the SSL certificate for each LDAP server.

If your LDAP server requires mutual authentication, which requires the client to present a certificate in addition to the server, you must also provide your LDAP server’s client certificate in a Java keystore type certificate.

Certificate criteria

A valid certificate must meet these criteria:

• The certificate can have a key size up to 2048 bits.
• The certificate must have one of these file extensions:

<table>
<thead>
<tr>
<th>Extension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DER</td>
<td>The Distinguished Encoding Rules format is a binary message transfer syntax. This format also supports the .CER and .CRT file extensions.</td>
</tr>
<tr>
<td>CER</td>
<td>Certificate file extensions for certificates using the Distinguished Encoding Rules format.</td>
</tr>
<tr>
<td>CRT</td>
<td>Certificate file extensions for certificates using the Distinguished Encoding Rules format.</td>
</tr>
<tr>
<td>PEM</td>
<td>The Privacy Enhanced Mail format is a base-64 encoded DER certificate enclosed between &quot;-----BEGIN CERTIFICATE-----&quot; and &quot;-----END CERTIFICATE-----&quot; text strings.</td>
</tr>
</tbody>
</table>

Certificate trust

By default, your instance trusts only certificates from a Certificate Authority (CA) recognized in the Java Virtual Machine (JVM). In this case, your instance does not trust self-signed certificates.
Generate an LDAP client certificate

Generate an LDAP client certificate for mutual authentication using OpenSSL. The final output is a PKCS#12 certificate stored within a Java keystore.

Role required: admin

See the OpenSSL documentation for more information about generating certificates. These steps assume you have access to OpenSSL.

Enter these commands in a command line interface.

1. Generate a self-signed client certificate.
   For example, this command creates a client certificate test1-cert.crt based on the test1-key.key private key.
   
   ```
   openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout test1-key.key -out test1-cert.crt
   ```

2. Convert both the certificate file and private key to PKCS#12 (a file with a .pfx or .p12 extension).
   For example, this command converts the client certificate and private key to a PKCS#12 certificate called test1-certificate.pfx.
   
   ```
   openssl pkcs12 -export -out test1-certificate.pfx -inkey test1-key.key -in test1-cert.crt
   ```

3. Generate the Java Key Store and import the pkcs12 file into it.
   For example, this command imports the certificate to the test1.jks Java keystore.
   
   ```
   keytool -importkeystore -srckeystore test1-certificate.pfx -srcstoretype PKCS12 -destkeystore test1.jks
   ```

4. Upload the certificate in the keystore file (test1.jks) to the instance.

Upload a certificate to an instance

Generate a server certificate

You can use keytool to generate a new Java keystore file, create a certificate signing request (CSR), and import the private key, public certificate pair, and signed certificates into the keystore.

Role required: admin

See the Java keytool documentation for more information on generating keys and CSRs.

Enter these commands in a command line interface:

1. Generate a Java keystore and key pair.
   For example, this command creates a keystore called my.keystore and generates a private key called mydomain within the keystore.
   
   ```
   keytool -genkey -alias mydomain -keyalg RSA -keystore my.keystore
   ```

2. Generate a CSR for an existing Java keystore.
   For example, this command generates a CSR called mydomain.csr or the mydomain key.
   
   ```
   keytool -certreq -alias mydomain -keystore my.keystore -file mydomain.csr
   ```
3. Import a root or intermediate certificate authority, or CA, certificate to the Java keystore. For example, this command imports the CA certificate for Thawte. This command assumes that Thawte was the CA that signed the CSR.

```
keytool -import -trustcacerts -alias root -file Thawte.crt -keystore my.keystore
```

4. Import a signed primary certificate to the Java keystore. For example, this command imports the signed certificate mydomain.crt into the keystore.

```
keytool -import -trustcacerts -alias mydomain -file mydomain.crt -keystore my.keystore
```

5. Upload the certificate in the keystore file (my.keystore) to the instance.

**Upload a certificate to an instance**

### Upload a certificate to an instance

You can add a certificate to the instance from the Certificates module.

Role required: admin

When a certificate is updated on the ADFS server, you also need to upload an updated certificate to the instance.

1. Navigate to **System Definition > Certificates**.
2. Click **New**.
3. Fill in the following fields (see table).

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify a unique name for the certificate.</td>
</tr>
<tr>
<td>Expiration notification</td>
<td>[Optional] Select whether you want to send a notification when the certificate is about to expire.</td>
</tr>
<tr>
<td>Active</td>
<td>Select whether the instance should use this certificate for secure communications and signing requests.</td>
</tr>
<tr>
<td>Short Description</td>
<td>[Optional] Enter a text description of the certificate such as the requester or server name.</td>
</tr>
<tr>
<td>Format</td>
<td>Select the certificate format. The instance supports the PEM and DER formats.</td>
</tr>
<tr>
<td>Type</td>
<td>Select the certificate container. The instance recognizes certificates from trust stores, Java keystore, and PKCS#12 keystores.</td>
</tr>
<tr>
<td>PEM Certificate</td>
<td>Enter the base-64 encoded PEM-formatted text containing the DER certificate. The instance decodes the certificate to populate the <strong>Valid from</strong>, <strong>Expires</strong>, <strong>Expires in days</strong>, <strong>Issuer</strong>, and <strong>Subject</strong> fields.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

During the upload, the module extracts and displays the certificate's read-only properties in these fields:

- Valid from date
- Expiration date
- Issuer
- Subject of the certificate
5. Click **Validate Stores/Certificates** to check if the certificate is correct. If the instance encounters any errors with the certificate or keystore, it displays an error message.

**Upload a trusted server certificate**

By uploading the service provider's trusted server certificate, the instance ensures it is connecting to a valid and secure service.

Role required: admin

The instance validates outbound Web Service calls by using the certificate provided by the service provider.

1. Create a new Certificate record with the type "Trust Store Cert".
2. Do one of the following actions:

- Attach the service provider’s DER formatted certificate.

- Copy and paste the service provider’s PEM format certificate into the **PEM Certificate** field.
**Web service security**

Enforce security using basic authentication, mutual authentication, or WS-Security.

**Basic Authentication**

To enforce basic authentication on each request for a WSDL document or posting of SOAP messages, you may set the property `glide.basicauth.required` to `true`. If you do so, each WSDL or SOAP request would have to contain the "Authorization" header as specified in the Basic Authentication protocol. Because the request is non-interactive, the **Authorization** header is always required during a request.

Supplying basic authentication information whether or not it is required has the added advantage that the data created or updated as a result of the Web Service invocation is done on behalf of the user supplied in the basic authentication credentials. As an example, when creating an Incident record, the journal fields have the user id of the basic authenticated user, instead of the default **Guest** user.

To make the authorization header ignore the capitalization rules, use the `glide.security.script.include.name.case.insensitive.list` property. You can modify this property in the System Properties [sys_properties] table and add the script includes that are necessary to process the authentication. By default, this property has these values:

- BasicAuth
- CustomAuth

Add other script includes as needed.

To supply basic authentication when using Perl and the SOAP::Lite libraries, you can implement the following function:

```perl
sub SOAP :: Transport :: HTTP :: Client :: get_basic_credentials { return 'user_name' => 'password' ; }
```

- When using C# .NET VS 2005 or older, you can take advantage of the Credentials object, for example:

  ```csharp
  
  service . ServiceNow proxy = new service . ServiceNow ( ) ;
  service . get getService = newservice . get ( ) ;
  service . getResponse getServiceResponse = new service . getResponse ( ) ;
  
  try {
  proxy . Credentials = cred ;
  getService . sys_id = "bf522c350a0a140701972dbf876f1610" ;
  getServiceResponse = proxy . get (getService ) ; catch (Exception ex )
  }
  ```

- When using C# .NET VS 2008, you can take advantage of the ClientCredentials object, for example:

  ```csharp
  Demo_Incident. ServiceNowSoapClient client = new Test08WebService .
  Demo_Incident. ServiceNowSoapClient ( ) ;
  client . ClientCredentials . UserName . Username = "admin" ;
  ```
Then in your app.config file look for the following and change "None" to "Basic":

```
<transport clientCredentialType= "None" proxyCredentialType= "None" realm= "" />
```

- When using VB .NET taking advantage of the Credentials object would look like the following:

```vbnet
Sub Main()
    Dim cred As New System.Net.NetworkCredential( "user_name", "password")
    Dim proxy As New VB_Democm.incident.ServiceNow
    Dim getIncident As New VB_Democm.incident.get
    Dim getResponse As New VB_Democm.incident.getResponse
    proxy.Credentials = cred
    getIncident.sys_id = "[your sysID here]"
    getResponse = proxy.get(getIncident)
End Sub
```

The resulting response when Basic Authentication is turned on and no credentials are supplied looks like this:

```html
<html> <head > <title >Apache Tomcat/5.0.28 - Error report </title > <style > <!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;} A {color&nbsp;:
black;} A.name {color&nbsp;: black;} HR {color&nbsp;: #525D76;}-->
</style > </head > <body > <p >HTTP Status 401 -
</p>
<p ><b >type </b> Status report </p>
<p ><b >message </b> <u >This request requires HTTP authentication ().</u>
</p>
<p ><b >description </b> "1" noshade = "noshade" > <p >"1" noshade = "noshade" > <p >"1" noshade = "noshade" > <p >Apache Tomcat/5.0.28 <= h3 > </body ></html>
```

### Setting up mutual authentication

Mutual authentication establishes trust by exchanging secure sockets layer (SSL) certificates.

Before connecting to a server, the client requests an SSL certificate. The server responds by requesting that the client send its own certificate. Both respond by validating the certificates and sending acknowledgments before initiating an HTTPS connection.

Administrators do the preliminary work of setting up a keystore and generating certificates before certification requests are fulfilled.

**Warning:** This feature enables mutual authentication on outbound https connections and inbound https connections.
Creating the Key Store

The instance currently supports uploading a Java keystore file to contain the private key, public certificate pair, and its signed certificates.

The following steps use commands that allow you to generate a new Java Keytool keystore file, create a certificate signing request (CSR), and import certificates. Any root or intermediate certificates need to be imported before importing the primary certificate for your domain. Type these commands in a command line interface.

1. Generate a Java keystore and key pair.
   ```
   keytool -genkey -alias mydomain -keyalg RSA -keystore my.keystore
   ```

2. Generate a CSR for an existing Java keystore.
   ```
   keytool -certreq -alias mydomain -keystore my.keystore -file mydomain.csr
   ```

3. Import a root or intermediate certificate authority CA certificate to an existing Java keystore.
   ```
   keytool -import -trustcacerts -alias root -file Thawte.crt -keystore my.keystore
   ```

4. Import a signed primary certificate to an existing Java keystore.
   ```
   keytool -import -trustcacerts -alias mydomain -file mydomain.crt -keystore my.keystore
   ```

Setting up the Key Store

Now that the key store has been created, it can be uploaded to the Certificates table. On the System Definition > Certificates page, click New and set the following fields:

- Enter a certificate Name.
- Store the key store as Active.
- Set Type = Java Key Store.
- Provide a Key store password. This is the password that was used to create the keystore.

Click Submit to create the Java Key Store entry.
Specifying a Trusted Server Certificate

During an outbound SSL connection, which is an HTTPS Web Service call, it is possible to specify a certificate provided by the service provider that ensures the validity of the service provider during the SSL connection. For example, a browser attempting to connect to a secure service which identifies itself by a certificate.

By uploading the trusted server certificate, ServiceNow ensures that the service it is connecting to is valid and secure.

Create a new Certificate entry with the type of "Trust Store Cert" and attach a DER formatted certificate, or copy and paste its PEM format into the **PEM Certificate** field.

Processing Mutual Authentication Requests

**Certificate Exchange**

- When a client requests the server certificate for authentication, a certificate signing request (CSR) is generated.
- To respond to a CSR, the server generates two unique cryptographic keys: A public key, which is used to encrypt messages to the server and a private key, which is used to decrypt messages. Both keys are kept in the Key Store.
- Keys are used to decrypt the client secure messages so they can be read by the server. Any outgoing connection that is going to be HTTPS verifies the certification by checking the Key Store, offering its public certification, and uses the trust store certificates to verify mutual trust back.
- To complete the secure link between the client and the server, the server matches the certificate to the corresponding private key. Because only the server has access to the private key, the server can decrypt the data from the client.

Here is an example of a command that registers MYHTTPS with the `com.glide.certificates.DBKeyStoreSocketFactory` socket factory on port 443. The database key store factory is used during the SSL exchange process to offer a client certificate for mutual authentication.

```bash
glide.httpclient.protocol.myhttps.class = "com.glide.certificates.DBKeyStoreSocketFactory"
glide.httpclient.protocol.myhttps.port = "443"
```
Having the above configuration affects any outbound myhttps://host.domain.com/target URL to use the custom socket factory and exchange certificates during SSL.

**Note:** Overriding the default HTTPS protocol socket factory affects every outbound HTTPS connection. This is usually undesirable.

The server responds by sending a certificate. Is this a certificate that the client accepts? If yes, a message is sent to the server accepting the certificate and a secure channel is initiated. If the certificate is not accepted, it may mean that the root authority is needed for certification.

**WS-Security**

Support for WS-Security 1.1 in the form of WSS X.509 Token Profile and WSS Username Token Profile is available for incoming SOAP requests.

The configuration to use WS-Security is separate from the requirement to enforce Basic Authentication, and is enforced when the SOAP envelope contains the WS-Security headers.

**WS Security Profiles**

The WS Security Profile module lists the WS-Security profiles that are currently in effect. The Order of the profiles indicates the order of authentication that is checked, all profiles are checked during the incoming SOAP request, when a profile fails authentication, it does not execute the next one in order. The Bind session check box indicates which profile to use to assume the session’s identity, there can only be one “bound” session.

**WS Security List**

**WSS X.509 Token Profile**

Use the X.509 authentication framework as defined by the Web Services Security: SOAP Message Security specification. An X.509 certificate specifies a binding between a public key and a set of attributes that includes (at least) a subject name, issuer name, serial number, and validity interval. An X.509 certificate is used to validate a public key that is used to sign the incoming SOAP message. Upload the certificate in the Certificate module and reference it in the X509 Certificate field. If this is a bound session, select the user to impersonate when the WS-Security authentication succeeds.

See the following document: [http://www.oasis-open.org/committees/download.php/16785/wss-v1.1-spec-os-x509TokenProfile.pdf](http://www.oasis-open.org/committees/download.php/16785/wss-v1.1-spec-os-x509TokenProfile.pdf)
WS x509

WSS Username Token Profile

In addition to specifying the X.509 Token Profile, a UsernameToken can also be supplied in the SOAP request. A UsernameToken is used as a means of identifying the requester by "username", and optionally using a password (or shared secret, or password equivalent) to authenticate that identity to the instance. The UsernameToken profile cannot be used independent of the X.509 Token Profile currently.

1. Authenticate using the Username of the incoming SOAP request to lookup a User by the specified User field to match UserName value. The password value in the incoming Username Token is used to authenticate the request. When the Bind session option is selected, the user that authenticates successfully is used for the session.

2. Authenticate using a separate pair of user name / password that is unrelated to users in the User table. When the Bind session option is selected, the user that is specified in the Run as user field is used for the session.

Example WS-Security SOAP Envelope Headers

Note:

This sample has been formatted with line returns to fit the content into the frame.

```xml
HTML sanitizer

Remove unwanted code and protect against security concerns such as cross-site scripting attacks by sanitizing HTML markup in HTML fields and translated HTML fields.

The HTML sanitizer works by checking the built-in inclusion list for markup that you always want to preserve. The sanitizer provides the HTMLSanitizerConfig script include that administrators can use to modify the built-in inclusion list. Items can also be added to the exclusion list, which overrides the inclusion list, to remove HTML markup.

The following types of items can be added to inclusion and exclusion lists:

- Global attributes
- Any HTML elements

Note: By default, URL attributes like href and src support only these protocols:
- http
- https
- mailto
- data

For example:

```
<a href="https://community.servicenow.com/community">Now Community</a>
```
Note: To learn more about the glide.html.sanitize_all_fields property that controls use of the HTML sanitizer, see HTML sanitizer (instance security hardening) in Instance Security Hardening Settings.

Configure urlAttributes and the protocols

You can configure urlAttributes and their protocols in the HTMLSanitizer script include. For example:

```javascript
HTML_WHITELIST : {
    urlAttributes: { "protocols" : [ "file", "notes" ] },
    - -
    - -
}
```

Because notes is in the inclusion list in the example above, this URL is not sanitized:

```html
<a title="Lotus" href="Notes://ABC/X575C90019DE33/
ABC594DCB76D86EB4925653E0011C4C1/Z290B7E2D33964749257EEA003456FD">Lotus</a>
```

The Default Inclusion List

```javascript
BUILTIN_HTML_WHITELIST :{
    globalAttributes:{ attribute:["id","class","lang","title","style"],
                        attributeValuePattern:{}},

    label:{ attribute:["for"],

    font:{ attribute:["color","face","size"],

    a:{ attribute:["href","nohref","name","shape"],

    img:{ attribute:
        ["src","name","alt","border","hspace","vspace","align","height","width"],

    table:{ attribute:
        ["border","cellpadding","cellspacing","bgcolor","background","align","no resize","height","width","summary","frame","rules"],

    th:{ attribute:
        ["background","bicolor","abbr","axis","headers","scope","nowrap","height","width","align","off","char","colspan","rowspan"],

    td:{ attribute:
        ["background","bicolor","abbr","axis","headers","scope","nowrap","height","width","align","off","char","colspan","rowspan"],

    tr:{ attribute:["background","height","width","align","valign","char off","char"],

    thead:{attribute:["align","valign","char off","char"]},

    tbody:{attribute:["align","valign","char off","char"]},

    tfoot:{attribute:["align","valign","char off","char"]},
```

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Enable HTML sanitizer

The HTML sanitizer provides a property to enable or disable the sanitizer for all HTML fields in the system.

Role required: admin

By default, the property is set to true for new instances.

1. In the navigation filter, enter `sys_properties.list`.
2. Set the properties `glide.html.sanitize_all_fields` and `glide.translated_html.sanitize_all_fields` to true.

   **Note:** To learn more about this property, see HTML sanitizer (instance security hardening) in Instance Security Hardening Settings.

   If the properties do not exist in the System Properties table, you can add them.

Configure HTML sanitizer

You must modify a script include to make configuration changes to the HTML sanitizer.

Role required: admin

1. Navigate to System Definition > Script Includes.
2. Open HTMLSanitizerConfig.
3. To add items to the exclusion list, use the HTML BLACKLIST class. To add items to the inclusion list, use the HTML WHITELIST class.

   Use this format:

   ```
   HTML_XXXXLIST :{
       globalAttributes :{
           attribute:[attribute-name1,...],
           attributeValuePattern:{ attribute-name2:attribute-value-regex-pattern,...}
       },<html-element-name>:{// Same as Above},----}
   ```

   • **globalAttributes** contains attribute or attributeValuePattern items that are applicable globally for all the HTML elements.
   • **attribute** is a comma-separated list of attributes.
   • **attributeValuePattern** is a dictionary of attribute to attribute-value-regex-pattern pairs. The attribute-value-regex-pattern is a regular expression which has to match the attribute value.

   Consider the following example:

   ```
   HTML_WHITELIST:{
       globalAttributes:{
           attribute:["id","name"],},
       img:{
           attribute:["style","align"],
   ```
It adds the following items to the inclusion list:

- The global attributes id and name. This is a list of strings that can be applied globally to all the elements.
- The img element where the attributes are style and align.
- The img element where the source attribute of the image is a file with the .jpeg extension. This is an example of a regular expression pattern that matches an attribute value.
- The iframe element.

**Enable sanitization on individual fields**

You can use field attributes to enable or disable the sanitizer on individual fields.

Role required: admin

You need to first set the sanitizer property to false, and then enable the sanitizer on a per-field basis for any form.

1. Navigate to the sys_properties table and set the `glide.html.sanitize_all_fields` to **false**. This disables the sanitizer for all HTML fields in the system.
2. Navigate to the form that contains the HTML field.
3. Right-click the HTML field label, and select **Configure Dictionary**. The Dictionary Entry form opens for the HTML field.
4. Enter one of the following in the Attributes field:
   - To disable sanitization enter `html_sanitize=false`
   - To enable sanitization enter `html_sanitize=true`
5. Click **Update**.
6. To enable the HTML sanitizer for translated HTML fields, set the `glide.translated_html.sanitize_all_fields` property is **true**.

**Enable HTML Sanitizer logging**

When the HTML sanitizer removes elements or attributes, they are added to the system log.

You can review these sanitized elements by adding `/syslog_list.do?sysparm_query=source%3DHTMLSanitizer` to your instance URL.

1. To review these sanitized elements add `/syslog_list.do?sysparm_query=source%3DHTMLSanitizer` to your instance URL.
2. To enable or disable logging, add the `glide.html_sanitize.discarded_log.enable` property to the system properties and set the value to **true** (enabled) or **false** (disabled). This property is **true** by default.

**Encryption on the Now Platform**

Encryption is the process of scrambling data so that only authorized parties can understand information. Use encryption to protect sensitive information.

Encryption keys, formed from strings of bits used with an encryption algorithm, convert plaintext data into ciphertext that remains indecipherable to anyone who does not have access to the correct key.
Encryption gains its security benefits from the combination of the strength of the algorithms used and key management. ServiceNow key management makes encryption an effective control that is based on NIST 800-57 guidelines.

**Encryption on the Now Platform**

Information for all data may not require encryption. Consider the additional time required to process large amounts of data supported across every application. Therefore, determine the supported fields to be encrypted and use any of these Now Platform options:

**Platform Encryption**

Platform Encryption utilizes the Key Management Framework (KMF), which provides key-protection and key lifecycle management for application-level field encryption. All keys are protected with a key-wrapping hierarchy ultimately rooted in FIPS 140-2-L3 Hardware Security Modules (HSM). In addition to allowing for segregation of duties, KMF allows lifecycle management of the keys that encrypt and decrypt data on your instance to NIST 800-57 best practice. A subscription is required to enable Platform Encryption. For more information, see Platform Encryption and Key Management Framework (KMF).

**Encryption Support**

Encryption Support, also known as Column Level Encryption (CLE), is a built-in feature which permits encryption of string, date, date/time, or attachment fields using AES-128 or AES-256 in encryption contexts. You can encrypt existing non-system string fields or newly created fields. Column Level Encryption (CLE) contexts permit and deny access to encrypted data based on user role. See Encryption Support for more information.

**Edge Encryption**

Edge Encryption encrypts sensitive data on your company premises before sending it over the internet to your instance (encrypted in transit), where it remains encrypted at rest. Also referred to as ‘client-side’ encryption, Edge requires all bi-directional user traffic to pass through proxies that are maintained on your infrastructure. You have the full control over your key management, as the keys are stored within your proxy on your infrastructure and ServiceNow cannot decrypt your ciphertext to access your keys.

For more information, see Edge Encryption.

**Database Encryption**

Database Encryption enables all data to be protected with symmetric AES-256 encryption, whether the database is online or offline. From the Now Platform perspective, all data flows in decrypted. This capability is available for all supported releases. For more information, see Database encryption and full-disk encryption.

**Key Management Framework (KMF)**

The ServiceNow Key Management Framework (KMF) provides a secure and comprehensive interface for instance-side cryptographic key management services.

**Explore**

- Understanding the Key Management Framework
- Cryptographic module overview
- Cryptographic purpose, algorithms, and key information
- Key management actions
- Key lifecycle states
- KMF roles

**Getting Started**

- Create a cryptographic module
- Create module access policy
- Create a cryptographic module lifecycle policy
- Configure and upload your customer supplied key

**Examples**

- Column encryption walkthrough

**Troubleshoot and Get Help**

- View declined cryptographic module usage requests
Understanding the Key Management Framework

The Key Management Framework (KMF) API/UX lets you fully customize and manage how cryptographic operations are performed on your ServiceNow instance.

In accordance with NIST 800-57 guidelines, KMF provides the following capabilities:

- Segregation of duties with dedicated roles for cryptographic management and operations, auditing, and integration
- Cryptographic modules enable configuration of cryptographic specifications for unique cryptographic purposes and key types
  - Symmetric key: Encryption and decryption, key wrapping and unwrapping, and authentication
  - Asymmetric key: Digital signature generation and verification, encryption and decryption, key wrapping and unwrapping
- Key lifecycle management to generate, rotate, revoke, and suspend keys, including support of several key lifecycle states
- Enforcement of access controls (module access policies), ensuring that only specified users are granted access to the cryptographic modules
- Key protection: FIPS 140-2-L3 hardware root of trust (RoT), Public Key Infrastructure (PKI), key hierarchy, and envelope encryption
- Auditing that includes key usage statistics

KMF activation

KMF is active by default.

Note: KMF does not support domain separation, but can be used with on-premise instances.

In order to use Platform Encryption or Column Level Encryption contexts, one of these plugins must be active:

Platform Encryption (com.glide.now.platform.encryption)

Platform Encryption uses the Platform Encryption with Key Management Framework through cryptographic modules and module access policies. For more information on obtaining Platform Encryption see Platform Encryption and Activate Platform Encryption.

Encryption Support (com.glide.encryption)

Encryption Support, also known as Column Level Encryption, uses encryption contexts based on role. For more information on Encryption Support see Encryption Support.

It is recommended that you use Platform Encryption, which is the successor to Encryption Support.

How KMF works

This graphic shows you the components that comprise KMF:

- The cryptographic module is the basis for defining the encryption method.
- The cryptographic specification is a configuration that defines an algorithm for encryption.
• The specification also lets you define the key for the module. Use a ServiceNow key or bring your own customer-supplied key using Platform Encryption.
• A module access policy is an instance-level policy that places limits on cryptographic modules. An example is setting the duration for the key validity.

For more information on KMF, start with Cryptographic module overview.

The Key Management Framework (KMF) introduces specific roles for cryptographic module and key management related configurations. Only KMF Admins can assign users to other KMF roles. See KMF roles for more information.

For more information on the encryption framework that replaces CLE, see Platform Encryption.
Cryptographic module overview
Cryptographic modules are the centerpiece of KMF. They define the specific cryptographic mechanisms used for cryptographic operations for a given use case.

An example is using AES-CBC with a 256-bit symmetric key to encrypt and decrypt data within an HR application, using Platform Encryption. Cryptographic modules also support best-practice key lifecycle management (generate, rotate, renew, revoke, suspend) and are the basis for defining the encryption method. See Key lifecycle states for details.

Logically, cryptographic modules are composed of the following components:

- Cryptographic specification: Defines cryptographic purpose and algorithms.
- Cryptographic keys: Define as either a ServiceNow key or with Platform Encryption, use your own customer-supplied key.
- Module access policies and module policy exceptions: Instance-level definition of cryptographic modules, such as how long the key is valid.

The following screen shows these high-level components in a cryptographic module:
Cryptographic module components

How KMF works

Cryptographic purpose and algorithms encompass algorithm definition, which includes algorithm (for example, AES), operation mode (for example, GCM), key size (for example, 128-bit), and cryptographic purpose. A default cryptographic specification template is provided out-of-the-box with recommended NIST algorithms and key sizes for configuration. See Cryptographic purpose, algorithms, and key information for details.
The cryptographic keys component involves the creation of the cryptographic module’s key. Generate cryptographic keys on the instance by ServiceNow or import customer supplied keys. This component also includes lifecycle definition and key management actions (for example, rotate).

Module access policies are the access controls mechanisms that can be applied to the cryptographic modules.

- Encryption Support: Module access policies can be based on scope (basic), role, or script.
- Platform Encryption: Policies can be based on scope (basic) or KMF Resource Exchange.

Refer to Create module access policy for details.

Module access policies can be used across multiple modules. Refer to Multiple modules access policy for details.

**Instance level keys in KMF**

The KMF architecture introduces a specific key structure built with security in mind. Using a Hardware Security Module (HSM), KMF uses envelope encryption to ensure that all platform keys under KMF management are protected through a chain of keys. Customer Data Encryption Keys (CDEKs) created by KMF are also included.

At the instance level, KMF defines several internal keys that are used internally for varying cryptographic purposes throughout the platform.

<table>
<thead>
<tr>
<th>Key</th>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root Key (RK)</td>
<td>HSM</td>
<td>Root key used to decrypt the IRK.</td>
</tr>
<tr>
<td>Instance Root Key (IRK)</td>
<td>HSM</td>
<td>Unique per instance, the IRK is used to envelope encrypt several instance internal keys.</td>
</tr>
<tr>
<td>Instance Keyed-hash Message Authentication Code Key (HMAC IHK)</td>
<td>Instance</td>
<td>Unique per instance, the IHK is used internally for HMAC purposes.</td>
</tr>
<tr>
<td>Instance Key Encryption Key (IKEK)</td>
<td>Instance</td>
<td>Unique per instance, the IKEK is used internally to envelope encrypt key material.</td>
</tr>
<tr>
<td>Instance Asymmetric Encryption Key (IAEK)</td>
<td>Instance</td>
<td>Unique per instance, the IAEK is used internally for asymmetric encryption purposes.</td>
</tr>
<tr>
<td>Instance Signature Key (ISK)</td>
<td>Instance</td>
<td>Unique per instance, the ISK is used internally for signing purposes.</td>
</tr>
<tr>
<td>Customer Data Encryption Key (CDEK)</td>
<td>Instance</td>
<td>Generated by customers, encryption keys created through KMF are envelope encrypted by the IKEK.</td>
</tr>
<tr>
<td>Instance Data Replication Data Encryption Keys (IDR DEKs)</td>
<td>Instance</td>
<td>Specific encryption keys use for the Instance Data Replication (IDR) process.</td>
</tr>
</tbody>
</table>

The instance root key (IRK) and instance internal key (IKEK) are unique per instance. The figure below provides an overview of the key relationships.

**Note:** The preceding table and the following figure show only a few examples of customer/app keys that are managed and protected by KMF.
Store on HSM

Root Key

Instance Root Key

Instance Internal Keys

HMAC key

IKEK

IAEK

ISK

Customer/App Keys

Module keys

IDR DEKs

Unique per Instance
Envelope encryption is the practice of encrypting a key with another key. The following figure provides an example of the envelope encryption. Here, CDEKs are envelope encrypted by the IKEK, which in turn is envelope encrypted by the IRK, which is finally envelope encrypted by the RK. Since the IRK is only be accessed by the HSM, the IKEK must be uploaded for decryption.

Cryptography purpose, algorithms, and key information
Cryptographic specifications can be tailored to a specified cryptographic purpose, covering both asymmetric and symmetric key-based cryptographic operations. Selection of a cryptographic purpose offers further choices, namely to a set of supported algorithms and key length configurations.

<table>
<thead>
<tr>
<th>Cryptographic Purpose</th>
<th>Algorithm</th>
<th>Key Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asymmetric Data Decryption</td>
<td>RSA</td>
<td>Asymmetric – 2048-bit, 3072-bit, and 4096-bit key</td>
</tr>
<tr>
<td>Asymmetric Data Encryption</td>
<td>RSA</td>
<td>Asymmetric – 2048-bit, 3072-bit, and 4096-bit key</td>
</tr>
<tr>
<td>Asymmetric Key Unwrapping</td>
<td>RSA</td>
<td>Asymmetric – 2048-bit, 3072-bit, and 4096-bit key</td>
</tr>
<tr>
<td>Asymmetric Key Wrapping</td>
<td>RSA</td>
<td>Asymmetric – 2048-bit, 3072-bit, and 4096-bit key</td>
</tr>
<tr>
<td>Signature Generation</td>
<td>RSA</td>
<td>Asymmetric – 2048-bit, 3072-bit, and 4096-bit key</td>
</tr>
<tr>
<td>Signature Verification</td>
<td>RSA</td>
<td>Asymmetric – 2048-bit, 3072-bit, and 4096-bit key</td>
</tr>
<tr>
<td>Symmetric Authenticity</td>
<td>HMAC</td>
<td>Symmetric – 256-bit, 384-bit, and 512-bit key</td>
</tr>
<tr>
<td>Symmetric Data Encryption/Decryption</td>
<td>AES-CBC *</td>
<td>Symmetric – 128-bit, 192-bit, 256-bit key</td>
</tr>
<tr>
<td></td>
<td>AES-CFB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AES-OFB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AES-CTR</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AES-GCM**</td>
<td></td>
</tr>
<tr>
<td>Cryptographic Purpose</td>
<td>Algorithm</td>
<td>Key Information</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>Symmetric Key Wrapping/Unwrapping</td>
<td>AES-CBC *</td>
<td>Symmetric – 128-bit, 192-bit, 256-bit key</td>
</tr>
<tr>
<td></td>
<td>AES-CFB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AES-OFB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AES-CTR</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AES-GCM**</td>
<td></td>
</tr>
</tbody>
</table>

* AES-CBC (symmetric data encryption/decryption, symmetric key wrapping/unwrapping) supports equality persevering options. # utilizes AES-CBC. ** AES-GCM has data integrity built in.

The configuration of these parameters is covered in Create a cryptographic module.

**Key lifecycle states**

KMF supports several cryptographic key lifecycle states through the enforcement of specific allowable actions. For example, only keys that are in the active state can be used for their intended cryptographic purpose. The following table provides further detail on the varying key lifecycle states.

### Key lifecycle definitions

<table>
<thead>
<tr>
<th>Key lifecycle state</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>generated</td>
<td>Multiple keys can exist in the generated state for a given cryptographic specification in a cryptographic module. A generated key can be moved to an active state when no active key exists for the given cryptographic specification. The first key generated is automatically set to active.</td>
</tr>
<tr>
<td>active</td>
<td>There can be only one active key for a given cryptographic specification in a cryptographic module.</td>
</tr>
<tr>
<td>resume</td>
<td>Not a literal key state. A Resume Key UI action is available on suspended keys to move them back to an active state when no other active key exists for the given cryptographic specification in a module.</td>
</tr>
<tr>
<td>renewed</td>
<td>Considered an active key that can be renewed any number of times. A key can be renewed only when an expiration date is available, as it is a process of extending the lifecycle period of the key.</td>
</tr>
</tbody>
</table>

**Note:** The difference between the activation date and expiration date is calculated and the expiration date adjusted to the duration from the current day.

| rotated             | Key rotation results in deactivating the current active key and making another key active. The new active key based on either: (1) generation of a new key or (2) pointing to an existing (imported) key. Any active key can be rotated. |

**Note:** When generating a new key, the new key is set to active even though there are key(s) in a generated state for the given cryptographic specification.
### Key lifecycle state

<table>
<thead>
<tr>
<th>Key lifecycle state</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deactivated</td>
<td>Any active key can be deactivated. Multiple deactivated keys may exist in a cryptographic specification. For example, when a key is rotated the active key is deactivated. Deactivated keys cannot be used to generate new content, such as encrypting and signing, but may still be used to identify purposes of existing content: decryption, verification, etc. (until destroyed).</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Compromised and revoked keys are treated as deactivated keys.</td>
</tr>
<tr>
<td>suspended</td>
<td>There could be several keys in the suspended state for a given cryptographic specification in a cryptographic module. When the key is suspended, the key can be resumed and moved back to an active state if no other active key exists for that cryptographic specification for the given cryptographic module.</td>
</tr>
<tr>
<td>compromised</td>
<td>Several keys can exist in the compromised state for revocation in a given cryptographic specification. Any active or suspended key can be moved to a compromised state. Compromised keys cannot be used to generate new content, such as encrypting or signing, but may still be used to identify the purpose of existing content: decryption, verification, etc., until destroyed.</td>
</tr>
<tr>
<td>revoked</td>
<td>There could be several keys in revoked state for a given cryptographic specification. Any active or suspended key can be moved to the revoked state. Revoked keys cannot be used to generate new content, such as encrypting or signing, but may still be used to identify the purpose of existing content: decryption, verification, etc., until destroyed.</td>
</tr>
<tr>
<td>destroyed</td>
<td>There could be several keys in a destroyed state for a given cryptographic specification in a cryptographic module. When a key is destroyed, the key can no longer be used for any cryptographic purposes as the key material is permanently deleted/destroyed. Any deactivated key can be destroyed using lifecycle automation when it has not been used in the designated timeframe. The default timeframe is three months, however this value is configurable.</td>
</tr>
</tbody>
</table>

### KMF roles

The Key Management Framework (KMF) introduces specific roles for cryptographic module and key management-related configurations.

**Important:**

To assign the KMF admin role, you must have both the admin and security_admin roles.

Use the KMF admin role to assign other KMF roles.
<table>
<thead>
<tr>
<th>Role</th>
<th>Role Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>KMF admin</td>
<td>sn_kmf.admin</td>
<td>The administrator within the KMF application for all KMF related functions. Only users with the KMF admin role can assign KMF roles. KMF cryptographic manager permissions are also inclusive in the KMF admin role.</td>
</tr>
<tr>
<td>KMF cryptographic manager</td>
<td>sn_kmf.cryptographic_manager</td>
<td>Assigned to a user by a KMF admin. KMF cryptographic managers can perform create, read, and update operations on cryptographic modules (association of keys to cryptographic usage and algorithm configurations) and module access policies. Also, KMF cryptographic managers can perform key management (generate, rotate, revoke) and life cycle operations.</td>
</tr>
<tr>
<td>KMF auditor</td>
<td>sn_kmf.cryptographic_auditor</td>
<td>Assigned to a user by a KMF admin. KMF cryptographic auditors can view cryptographic module information, key metadata, and life cycle-related details, as well as module access policy information.</td>
</tr>
<tr>
<td>KMF integrator</td>
<td>sn_kmf.cryptographic_integrator</td>
<td>Assigned to a user by a KMF admin. KMF integrators can access and utilize (integrate) cryptographic modules in third party applications.</td>
</tr>
</tbody>
</table>

Assign KMF roles

Administrators with the security_admin role can assign KMF admins, who in turn can assign other KMF roles.

Role required: admin and security_admin

You must elevate to the security_admin role before assigning the KMF admin role. For instructions, see .

1. Elevate to the security admin role.
2. Navigate to **User Administration > Users** and select the user you want to be the KMF admin.
3. Verify that the user already has the admin and security_admin roles. If not, click **Edit** under the Roles related list and add **admin** and **security_admin**.
4. Navigate to **System Security > Key Management Administration**.
5. Select the user you want to be KMF admin in the **Available Users** column and move them to the **Selected User(s)** column.

6. Click **Save**.
7. Navigate to **User Administration** > **Users** and select the user you just gave the KMF admin role to. That user now has the sn_kmf.admin role in the Roles related list. That user can now assign other KMF roles.

If you have the KMF admin role, follow these steps for assigning other KMF roles:

1. Navigate to **User Administration** > **Users** and select the user you want to have another KMF role, such as KMF Cryptographic Manager.
2. In the Roles related list, click **Edit** and select the KMF roles you want to assign the users. All KMF roles start with `sn_kmf`.

Configure field encryption settings to select key type

Cryptographic managers have the choice to use ServiceNow supplied keys for encryption or your own customer-supplied keys (CSK) with Platform Encryption on the Now Platform.

This topic applies to both Platform Encryption and Column Level Encryption. Customer-supplied keys are only available with Platform Encryption.

1. Navigate to **System Security > Field Encryption Settings**.
2. From the Field Encryption Settings, select either **ServiceNow Generated Keys** or **Customer Supplied Keys** from the **Key Source** list.

   ![Field Encryption Settings](image)

   **Field Encryption Settings**

   **Key Source**

   ![ServiceNow Generated Keys](image)

   ![Customer Supplied Keys](image)

   **Key source selection**

   This option changes the `com.glide.encryption.cle_kmf.key_source` property to either **ServiceNow Generated Keys** or **Customer Supplied Keys**.

3. Click **Save**.

   - If you are using your own customer supplied keys, see [Properties for customer supplied keys](#).
   - If you are using ServiceNow supplied keys, start creating your cryptographic module. See [Create a cryptographic module](#).

**Create a cryptographic module**

Create a cryptographic module to define the mechanisms used for cryptographic operations. After you create the module, create a cryptographic specification, define an algorithm for encryption, and generate the key.

Role required: `sn_kmf.cryptographic_manager`

This procedure describes options that are available with KMF out of box and options that should be used with Platform Encryption functionality. Platform Encryption functionality is available only when the `column_level_encryption`(com.glide.now.platform.encryption) plugin is active and `column_level_encryption` is the parent crypto module. See [Activate Platform Encryption](#) for more information on obtaining Platform Encryption.

1. Navigate to **Key Management > Cryptographic Modules > Create New**.
2. Complete the form:

   **Cryptographic Modules fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module name</td>
<td>Alphanumeric string referenced when running scripts</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Crypto spec template</td>
<td>Select the <strong>Default</strong> template to use to create the cryptographic module, as it contains mappings of many crypto purposes to crypto specifications and recommended algorithms.</td>
</tr>
<tr>
<td>Application</td>
<td>Read only. Click the information icon to open the Store Application information for the ServiceNow Key Management Framework.</td>
</tr>
<tr>
<td>Name</td>
<td>Read only. Crypto module name prepended with application scope name, &quot;sn_kmf.&quot;</td>
</tr>
<tr>
<td>Crypto module lifecycle state</td>
<td>The term lifecycle refers to the creation, use, and deactivation of a cryptographic module. Set to <strong>Draft</strong> initially during configuration. When using the module, set this field to <strong>Published</strong>. When selecting the Default template, the module is automatically set to Published.</td>
</tr>
<tr>
<td>Parent crypto module</td>
<td>There are internal modules that are provided base system:</td>
</tr>
<tr>
<td></td>
<td>• <strong>cm_glide_encrypter</strong>: Do not select this option.</td>
</tr>
<tr>
<td></td>
<td>• <strong>key_import</strong>: Use to import a key from web services</td>
</tr>
<tr>
<td></td>
<td>Choose a parent of the cryptographic module to define crypto module constraints.</td>
</tr>
<tr>
<td></td>
<td>• If only KMF is active and Platform Encryption is not active, do not select a parent.</td>
</tr>
<tr>
<td></td>
<td>• For Platform Encryption functionality, select <strong>column_level_encryption</strong> for Symmetric Data Encryption/Decryption with AES- CBC 256 for column and attachment encryption. See Cryptographic purpose, algorithms, and key information for details.</td>
</tr>
</tbody>
</table>

3. Click **Submit**.

After submitting successfully, you should see your cryptographic module in the Cryptographic Modules table. The system prepends the name with the scope to avoid conflict with other scoped applications. For example, if you created a module with the name `my_crypto_module` in the global application scope, the name is saved as `global.my_crypto_module`. 
4. Click the newly created cryptographic module to open the configuration options. On the **Crypto Specifications** tab, click **New**.

![Crypto Specifications](image)

**Crypto Specifications**

<table>
<thead>
<tr>
<th>Crypto Specifications</th>
<th>Module Keys</th>
<th>Module Policy Exceptions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Crypto module = test</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Key alias</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Crypto purpose</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5. Complete the Algorithm Definition Form:

This example shows AES CBC-256 encryption. If Platform Encryption is active and the parent module is `column_level_encryption`, only Symmetric Data Encryption/Decryption AES CBC-256 applies as the crypto purpose.

**Algorithm Definition fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crypto module</td>
<td>Read only. Name of the selected cryptographic module displays.</td>
</tr>
<tr>
<td>Crypto purpose</td>
<td>Select the purpose of this module. For example, you might use it for data encryption, signature generation, or key wrapping.</td>
</tr>
<tr>
<td>Algorithm</td>
<td>Type of algorithm used to accomplish the crypto purpose. Adjusts automatically based on the selected Crypto purpose.</td>
</tr>
<tr>
<td>Operation mode</td>
<td>This field may display based on the selected Crypto purpose.</td>
</tr>
<tr>
<td>Size</td>
<td>Select the bit size for encryption. 256-bit is the most secure size. This refers to Symmetric Data Encryption/Decryption and should be set when you enable the Platform Encryption and select <code>column_level_encryption</code> as the parent.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Hash</td>
<td>Select a hash. (Not supported with Platform Encryption functionality.</td>
</tr>
<tr>
<td>Equality preserving</td>
<td>Enables non-deterministic encryption. Selecting this option means that if the same data is encrypted more than once, the encryption is different each time. When non-deterministic encryption is enabled, you are unable to filter a list of encrypted data using equality comparison operators because the encoded data is always different.</td>
</tr>
<tr>
<td>Integrity</td>
<td>Integrity is provided when GCM operation mode is selected. This does not apply for Platform Encryption functionality.</td>
</tr>
</tbody>
</table>

6. Click **Next**.
7. The Lifecycle Definition list loads. View existing lifecycle definition data in the table.

**Lifecycle Definition fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crypto purpose</td>
<td>Read only. Purpose of this module.</td>
</tr>
<tr>
<td>Algorithm</td>
<td>Read only. Algorithm used to accomplish the crypto purpose. Refer to for algorithm details.</td>
</tr>
<tr>
<td>Crypto module</td>
<td>Read only. Name of the crypto module.</td>
</tr>
</tbody>
</table>

8. Optional: Define the lifecycle of the key in the list at the bottom of the same Lifecycle Definition form:

**Key Lifecycle fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applies to</td>
<td>Key that the lifecycle applies to.</td>
</tr>
<tr>
<td>For field</td>
<td>Field that the life cycle applies to.</td>
</tr>
<tr>
<td>Key type</td>
<td><strong>Relative</strong> lets you define a lifecycle policy relative to other lifecycle events such as generation, activation, and deactivation. <strong>Absolute</strong> lets you define an actual date for this lifecycle event.</td>
</tr>
<tr>
<td>Lifecycle default</td>
<td>Read only. Will display a value if set.</td>
</tr>
<tr>
<td>Order</td>
<td>Enter the order in which to process the crypto specification.</td>
</tr>
<tr>
<td>Relative duration</td>
<td>Number of years, months, or days the key is valid.</td>
</tr>
<tr>
<td>Relative duration type</td>
<td>Duration of the life cycle: <strong>Years</strong>, <strong>Months</strong>, or <strong>Days</strong>.</td>
</tr>
<tr>
<td>Relative operation</td>
<td><strong>Before</strong> or <strong>After</strong>.</td>
</tr>
<tr>
<td>Relative to</td>
<td>Field the duration is relative to.</td>
</tr>
</tbody>
</table>

9. Optional: Click **Update**.
10. Click **Next**.
11. Complete the Key Origin form.
   See Generate a cryptographic key for details on using ServiceNow keys.
   If you are supplying your own keys for Platform Encryption, first Configure and upload your customer supplied key.

12. Click Next.
   It takes several seconds before the Key Creation form appears.

13. Click the Module Keys tab to view the key.

14. Set the Crypto module lifecycle state to Published.

Create module access policy

**Configure key lifecycle states**

After you have created a cryptographic specification, you can configure the lifecycle actions for the keys in your instance.

Role required: kmf_crypto_admin

1. Navigate to Key Management > Cryptographic Modules > All.
2. Select the cryptographic module that controls the lifecycle of a key.
3. Click the key alias link for a crypto module in the Crypto Specifications related list.

4. Click the key from the Crypto Specifications tab.
   The Algorithm Definition page opens for the selected key.
5. Click Next.
   Default Key Lifecycle values are created based on the selected algorithms for the crypto specification.
6. Select a Key Lifecycle from the **Applies to** column on the Lifecycle Definition step for the crypto specification.

### Key Lifecycle configuration

**Key Lifecycle fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applies to</td>
<td>Read only. Key that the lifecycle applies to.</td>
</tr>
</tbody>
</table>
### Key lifecycle management "For field" values

**Field** | **Description**
--- | ---
For field | Select the type of control for the key that the lifecycle applies to.

**Type**
- Select if the valuation for the key lifecycle is a relative value or an absolute value:
  - **Relative**: Enter a value that depends on other data entries in the system, such as key generation, activation, and deactivation.
  - **Absolute**: Enter an exact value, such as a date.

**Lifecycle default** | Read only. Displays a value if set.

**Order** | Enter the sequence in which to process the key lifecycle state for the crypto specification.

**Relative duration type** | Duration of the lifecycle: **Years**, **Months**, or **Days**.

**Relative duration** | Number of years, months, or days the key is valid.

**Relative operation** | **Before** or **After**.

**Relative to** | Field the duration is relative to.

### Create module access policy

Module access policies are the access control mechanisms on cryptographic modules.

Role required: sn_kmf.cryptographic_manager
Note: Module access policies replace the role and user that were specified in encryption contexts.

This procedure describes options that are available with KMF out of box, and options that should be used with Platform Encryption functionality. Platform Encryption functionality is available only when the Platform Encryption (com.glide.now.platform.encryption) plugin is active and `column_level_encryption` is the parent crypto module. See [Activate Platform Encryption](#) for more information on obtaining Platform Encryption. The parent crypto module options are described in [Create a cryptographic module](#).

Policies can be based on scope (basic), role, script or resource exchange. For Platform Encryption functionality, only role and resource exchange are supported.

To use a cryptographic module, you must configure correct module access policies to grant the right access. Without an access policy associated with the cryptographic module, encrypted data is not visible to users (fields and columns in lists are blank).

In this image, you can see how a lack of an access policy on an encrypted field, which in this case is the Short Description field on the Incident table, hides the content from all users. With an access policy in place, users with the allowed role are able to see the encrypted data.
### Without correct access policy

<table>
<thead>
<tr>
<th>Incident</th>
<th>Date</th>
<th>Time</th>
<th>Description</th>
<th>Caller</th>
</tr>
</thead>
<tbody>
<tr>
<td>INC000002</td>
<td>07/22/2019</td>
<td>14:49:57</td>
<td>System Administrator</td>
<td></td>
</tr>
<tr>
<td>INC000003</td>
<td>12/05/2019</td>
<td>10:17:14</td>
<td>Help Desk</td>
<td>David Miller</td>
</tr>
<tr>
<td>INC000004</td>
<td>08/30/2019</td>
<td>02:09:14</td>
<td></td>
<td>David Miller</td>
</tr>
<tr>
<td>INC000005</td>
<td>08/31/2019</td>
<td>22:30:21</td>
<td></td>
<td>David Miller</td>
</tr>
<tr>
<td>INC000006</td>
<td>09/03/2019</td>
<td>03:15:00</td>
<td></td>
<td>David Miller</td>
</tr>
<tr>
<td>INC000007</td>
<td>09/26/2019</td>
<td>05:49:23</td>
<td></td>
<td>David Miller</td>
</tr>
</tbody>
</table>

### With correct access policy

<table>
<thead>
<tr>
<th>Incident</th>
<th>Date</th>
<th>Time</th>
<th>Description</th>
<th>Caller</th>
</tr>
</thead>
<tbody>
<tr>
<td>INC000001</td>
<td>07/29/2019</td>
<td>14:49:43</td>
<td>Assessment - FTI Accessor</td>
<td></td>
</tr>
<tr>
<td>INC000002</td>
<td>07/30/2019</td>
<td>14:50:57</td>
<td>System Administrator</td>
<td></td>
</tr>
<tr>
<td>INC000003</td>
<td>12/05/2019</td>
<td>10:17:14</td>
<td>Help Desk</td>
<td>David Miller</td>
</tr>
<tr>
<td>INC000004</td>
<td>08/30/2019</td>
<td>02:09:14</td>
<td></td>
<td>David Miller</td>
</tr>
<tr>
<td>INC000005</td>
<td>08/31/2019</td>
<td>22:30:21</td>
<td></td>
<td>David Miller</td>
</tr>
<tr>
<td>INC000006</td>
<td>09/03/2019</td>
<td>03:15:00</td>
<td></td>
<td>David Miller</td>
</tr>
<tr>
<td>INC000007</td>
<td>09/26/2019</td>
<td>05:49:23</td>
<td></td>
<td>David Miller</td>
</tr>
</tbody>
</table>

(Excerpt from ServiceNow documentation on encrypted incident short descriptions with and without access policies)
1. Navigate to **Key Management > Module Access Policies > All**.

When you create a cryptographic module, an auto-generated Module Access Policy is created and will be listed in the table.

2. Click **New**.

3. Complete the form.

Module Access Policies fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy name</td>
<td>Enter a name for the policy.</td>
</tr>
<tr>
<td>Crypto module</td>
<td>Click the search icon to select a module.</td>
</tr>
</tbody>
</table>
| Type                   | • **Basic**: Controls access by Scope.  
                          • **Script**: Control access by script.  
                          • **Role**: Controls access by user role.  
                          • **Resource Exchange**: Control access using the Resource Exchange.  
                          
                          For Platform Encryption functionality, you can select only the Role or Resource Exchange types.  
                          
                          If the parent module is not **column_level_encryption**, you can select any of type.                                                                                                                                                                                        |
| Target Scope           | Field is visible as an identifier for the **Basic** Type. Refers to the functionality/scope for the policy. Select the applications from the search menu.  
                          Target scope is not supported if the parent module is **column_level_encryption**.                                                                                                                                                                                                 |
| Target Role            | Field is visible as an identifier for the **Role** Type. Role to which this policy applies.  
                          Target roles are supported by both KMF and by Platform Encryption when the parent module is **column_level_encryption**.                                                                                                                                                              |
| Script Table           | These fields appear when you select Script as the type.  
                          Field is visible as an identifier for the **Script** Type. Select a table to which this policy applies. Document to which this policy applies. Select the **Table name** and then the related document for the policy.  
                          The first time a script calls a cryptographic module, access to the module is denied, and the developer receives an error. This gives you, the module owner, the ability to grant or refuse access to your module.  
                          Target scripts are not supported if the parent module is **column_level_encryption**. See Configure script access to encrypted data for details.                                                                 |
<p>| Resource Exchange      | These options appear when you select Resource Exchange the type.                                                                                                                                                                                                                   |
| Crypto Spec            |                                                                                                                                                                                                                                                                                                                                             |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approval Type</td>
<td>Resource exchange is supported by both KMF and by Platform Encryption when the parent module is <code>column_level_encryption</code>. Select the crypto specification, One-time or Recurring, and the URL of the target instance. See KMF Resource Exchange for more information.</td>
</tr>
<tr>
<td>Target Instance Host</td>
<td></td>
</tr>
<tr>
<td>Active</td>
<td>Select to activate the policy.</td>
</tr>
<tr>
<td>Result</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>StrictReject</strong> to reject access under all circumstances</td>
</tr>
<tr>
<td></td>
<td>• <strong>Reject</strong> to prevent users with the <strong>Target Role</strong> or <strong>Target Scope</strong> from accessing this crypto module unless another policy allows them access</td>
</tr>
<tr>
<td></td>
<td>• <strong>Track</strong> to permit access and monitor use of the module</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

5. Select the policy name (not the module name) associated with the cryptographic module you want to examine.

**Multiple modules access policy**
You can encrypt data using multiple cryptographic modules. If each module has its own access policy based on a role, for example, users with different roles can encrypt data on the same table but they can still be prevented from viewing each others encrypted data.

- **Note:** Only Platform Encryption on columns supports multiple modules. Attachment encryption does not.

1. Create multiple cryptographic modules and an access policy for each one.
   Make sure that you grant different roles to the different cryptographic modules through the access policies.

2. Navigate to **System Security > Field Encryption > Encrypted Field Configurations**.
   If you need more information on Encrypted Field Configurations, see Set encrypted field configurations.

3. In the **Type** field, you must select **Column**. Attachment encryption does not support multiple modules.
4. Select **Multiple Modules** in the **Method** field.

Set method to multiple modules

5. Select the **Table** and the **Column** in the table that you want to encrypt.
6. Click **Submit**.

Newly created data for the specified field is encrypted with the key of the relevant module. When a user with the role specified in module A's access policy writes to the specified table, the data is encrypted with module A's key. Only users with the same role can read the data.

Let's say that you want to encrypt the Short Description column on the Incident table. You would do the following:

1. Create two cryptographic modules A and B.
2. For each module, create a module access policy.
   
   For module A, give users with an HR role access. For module B, give users with a Sales role access.
3. Create an Encrypted Field Configuration record specifying the Short Description column on the Incident table, and make sure that you select **Multiple Modules** in the **Method** field.
4. Have two users, one with the HR role (user A) and one with the Sales role (user B), create an incident with a short description, and then have both users look at the list of incidents.

   The short description for the incident created by the user with the HR role is encrypted by the key for module A. Likewise, the short description for the incident created by the user with the Sales role is encrypted by the key for module B.

   Although all users with the HR and Sales roles have access to incidents, only a user with the HR role can decrypt and view the short description for those incidents created by user A, who had the HR role. Likewise, only users with the Sales role can decrypt and view the short descriptions for those incidents created by the user B, who had the Sales role.
Create a cryptographic module lifecycle policy

A cryptographic module policy is an instance-level policy that places limits on cryptographic modules, such as how long the key is good for. Create policies to safeguard cryptographic modules by limiting their exposure.

Role required: sn_kmf.cryptographic_manager

The more exposure a cryptographic key has, the more likely it can be compromised. Safeguard keys by limiting how long the keys can be used and who can use them.

The following features govern cryptographic modules:

- Instance policies set boundaries for the instance. For example, if you specify in the instance policies that the expiration date should never be more than two years after the activation date, you cannot use the lifecycle rules to set an expiration date five years after the activation date.
- Instance lifecycle templates allow you to set different policies for different keys. Templates offer default lifecycle rules for cryptographic modules so that they don't have to be re-created for every module. For example, you can set different expiration dates for symmetric data encryption keys than for public key wrapping keys.
• Lifecycle rules affect the keys directly. For example, if you specify in the lifecycle rules that the expiration date should be two years after the activation date, keys will expire two years after the activation date.

1. Navigate to **Key Management > Lifecycle Policies > Instance Policies**.
2. Click **New**.
3. Complete the form.

**Cryptographic Lifecycle Policies fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applies to</td>
<td>Read only. The key the lifecycle applies to.</td>
</tr>
<tr>
<td>Active</td>
<td>Select to activate the policy.</td>
</tr>
<tr>
<td>Policy condition</td>
<td>Conditional statements that specify when to activate, renew, deactivate, and destroy the cryptographic module.</td>
</tr>
<tr>
<td>Result</td>
<td><strong>Reject</strong> to revoke access to the cryptographic module, or <strong>Track</strong> to permit access and monitor use of the cryptographic module.</td>
</tr>
</tbody>
</table>

If you want to add exceptions to this lifecycle policy at the module level, see **Create module policy exceptions**.

**Create module policy exceptions**

Create a module policy exception to change the lifecycle policy of a key at the module level for an instance. The exception(s) applies only to that module and not to the entire instance.

Role required: **sn_kmf.cryptographic_manager**

For example, if the administrator configured symmetric keys to be limited to one year at the instance level, an exception can be made at the module level to be two years.

1. Navigate to **Key Management > Cryptographic Modules > All**.
2. Select the cryptographic module that will use the policy exceptions.
3. In the Cryptographic Module table, select the **Module Policy Exceptions** tab.
4. Click **New**.
5. Complete the form.

**Module Policy Exceptions fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crypto Module</td>
<td>Read only, name of the module selected.</td>
</tr>
<tr>
<td>Applies to</td>
<td>The specified key is auto-populated.</td>
</tr>
<tr>
<td>Key Type</td>
<td>Select the key type, as the exception policies are related to a specific key. Multiple exception policies can be created per crypto module.</td>
</tr>
<tr>
<td>Policy condition</td>
<td>Choose the qualifying conditions from the drop-down and complete the additional constraint criteria.</td>
</tr>
<tr>
<td>New criteria</td>
<td>Select additional policy conditions, as required.</td>
</tr>
<tr>
<td>Result</td>
<td>Select to <strong>Reject</strong> to reject usage of the key or <strong>Track</strong> to allow usage of it when the criteria is met.</td>
</tr>
</tbody>
</table>

6. Click **Submit** to be returned to the Cryptographic Module table.
Generate a cryptographic key

Generate an encryption key that converts data into ciphertext, which remains indecipherable to anyone who does not have access to the correct key. Cryptographic managers have the choice to use ServiceNow supplied keys or your own customer supplied keys (CSK) for encryption on the Now Platform.

Role required: sn_kmf.cryptographic_manager

See Configure field encryption settings to select key type to configure your instance to use either ServiceNow generated keys. For Platform Encryption see Properties for customer supplied keys to use your own customer-supplied key.

1. Navigate to Key Management > Cryptographic Modules > All.
2. Select the crypto module for the key generation and select the crypto specification.
3. Navigate to the Key Origin tab by clicking Next.
4. On the Key Creation form, click Generate Key.
   The crypto specification data is pre-populated based on previous information added and key origin configuration.
5. Review these read-only fields based on your configuration:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crypto Module</td>
<td>Name of the module.</td>
</tr>
<tr>
<td>Key alias</td>
<td>Name of the key.</td>
</tr>
<tr>
<td>Crypto purpose</td>
<td>Purpose of the module.</td>
</tr>
<tr>
<td>Origin</td>
<td>Populated based on field configuration settings. For customer supplied keys, refer to Wrap your customer supplied key</td>
</tr>
<tr>
<td>Algorithm</td>
<td>Algorithm used to accomplish the crypto purpose.</td>
</tr>
</tbody>
</table>

Generate key
6. Click **Generate Key** to initiate the creation of a key for this cryptographic module.
   
   Multiple keys can exist for a given cryptographic module, but, only one key can be active at a time. Refer to Key management actions for additional information.
   
   The algorithm definition screen will open. Select options for the key generation. Repeat this step to generate multiple keys for the selected crypto module.
   
   Secure information for the key is stored on the Module Keys tab.
   
   Access the existing keys by selecting a filter in the Module keys table. Select a key to perform key management actions.
   
   After you generate the key, the Cryptographic Module form reloads showing you the specification.

7. Click the **Module Keys** tab to view the key.

8. Set the **Crypto module lifecycle state** to **Published**.

Configure script access to encrypted data

Execute a script to run the cryptographic module policy for a cryptographic purpose.

Role required: sn_kmf.cryptographic_manager

For KMF, policies can also be based on scripts. When an access policy is triggered for script access, the back-end script can execute the module policy actions from the script.

**Note:** Platform Encryption supports module access policies based on role or resource exchange. Script access is not supported.

Scripts are used to analyze data. If an analyzed field is encrypted, a module access policy can be entered for that script so the encrypted field can be accessed from the script.

Cryptographic modules can support one or more encryption purposes, such as Asymmetric Data Decryption and Symmetric Data Decryption. Each cryptographic purpose requires the generation of an encryption key and defined cryptographic purpose.

The following are required to successfully execute an encryption script request:

- The referenced cryptographic purpose must be defined in the cryptographic module.
- There must be an active generated key for the cryptographic module.
- Set the Module Access Policy type to **script**.

Examples of uses are for business rules and Script Includes. This procedure uses a script for Business Rules.

1. Create a cryptographic module with the symmetric data encryption/decryption algorithm. Refer to Create a cryptographic module for details.

2. Navigate to **System Definition > Business Rules**.
3. Click **New**.
A business rule is a server side script that runs when a record is displayed, inserted, deleted, or when record is opened. Use business rules to automatically change values in form fields when the specified conditions are met. Click Add to add a new business rule.

Specify whether the business rule should run on insert or update. Use filter conditions to specify under which conditions the business rule should run.

- **When**:
  - Before INSERT
  - After INSERT
  - Before UPDATE
  - After UPDATE
  - Before DELETE
  - After DELETE

- **Filter Conditions**:
  - Add Filter Condition
  - Add "OR" Clause
  - Add "AND" Clause
  - Add "NOT" Clause
  - Add "LIKE" Clause
  - Add "IN" Clause

- **Rate Conditions**:

Submit
4. Complete the form:

**Business Rule fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the business rule.</td>
</tr>
<tr>
<td>Table</td>
<td>Select <em>Incident [incident]</em> from the drop-down list.</td>
</tr>
<tr>
<td>Application</td>
<td><em>Global</em> is selected by default</td>
</tr>
<tr>
<td>Active</td>
<td>Mark the rule as <em>Active</em>.</td>
</tr>
<tr>
<td>Advanced</td>
<td>Select the check box to display advanced options.</td>
</tr>
<tr>
<td>“When to run” tab</td>
<td>Enable <em>Insert</em> and <em>Update</em> fields.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>&quot;Advanced&quot; tab</td>
<td>Paste the following script text in line 3,</td>
</tr>
<tr>
<td></td>
<td>// Add your code here line:</td>
</tr>
<tr>
<td></td>
<td>var gc = global.GlideCryptoModule.getModule('global.acme_mod');</td>
</tr>
<tr>
<td></td>
<td>var value = 'test';</td>
</tr>
<tr>
<td></td>
<td>var encrypted = gc.encryptData(value);</td>
</tr>
<tr>
<td></td>
<td>gs.info('value: ' + value);</td>
</tr>
<tr>
<td></td>
<td>gs.info('Encrypted: ' + encrypted);</td>
</tr>
<tr>
<td></td>
<td>var decrypted = gc.decryptData(encrypted);</td>
</tr>
<tr>
<td></td>
<td>gs.info('Decrypted: ' + decrypted);</td>
</tr>
<tr>
<td></td>
<td>gs.info(decrypted == value);</td>
</tr>
</tbody>
</table>

Note: Refer to the "Business Rules Advanced Tab" image below for details.

```
function executeRule(current, previous) {
    var gc = global.GlideCryptoModule.getModule('global.acme_mod');
    var value = 'test';
    var encrypted = gc.encryptData(value);
    gs.info('value: ' + value);
    gs.info('Encrypted: ' + encrypted);
    var decrypted = gc.decryptData(encrypted);
    gs.info('Decrypted: ' + decrypted);
    gs.info(decrypted == value);
}
```

5. Click Submit.
6. **Navigate to Key Management > Module Access Policies > All.**

   **Note:** For additional information, refer to Create module access policy.

7. Click **New**.

8. Complete the form.

   **Module Access Policies fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy name</td>
<td>Enter a name for the policy.</td>
</tr>
<tr>
<td>Crypto module</td>
<td>Click the search icon to select a module with the symmetric data encryption/decryption algorithm.</td>
</tr>
<tr>
<td>Type</td>
<td>Select Script to control access by script.</td>
</tr>
<tr>
<td>Script Table</td>
<td>Select a value from the script table drop-down list. For this example, select Business Rule [sys_script].</td>
</tr>
<tr>
<td>Target Script</td>
<td>Select the script document for the policy. Select the Table name and then the related document for the policy. For this example, select the Business Rule that you created in previous steps. The first time a script calls a cryptographic module, access to the module is denied and the requester receives an error. The module owner can grant or refuse access to the module.</td>
</tr>
<tr>
<td>Active</td>
<td>Select to activate the policy.</td>
</tr>
<tr>
<td>Result</td>
<td>To give the script access to the module, select Track in the Result field.</td>
</tr>
</tbody>
</table>

9. Click **Submit**.

   The Module Access Policy for the script is available in the system.

A module access policy is automatically created when a script attempts to use a module. The module name is preceded with "AutoGen-". For example, the "Module-TestPolicy" module is listed as "AutoGen-Module-TestPolicy" in the Policy name column.

The Crypto Caller Policy form lists the caller policy you selected. The Target Scope field specifies the scope of the script attempting to use the module.

**View declined cryptographic module usage requests**
View cryptographic modules that rejected encryption requests made by scripts because of unsupported encryption mechanisms.

**Role required: sn_kmf.cryptographic_manager**

Cryptographic modules can support one or more encryption purposes, such as Asymmetric Data Decryption and Symmetric Data Decryption. Each cryptographic purpose requires the generation of an encryption key. Encrypted data can only be accessed based on the module access policy. If a script tries to use a cryptographic module for a purpose not defined in the module or without an encryption key, the script cannot access to the encrypted data. To successfully run a script to access encrypted data, create an encryption key for which the encryption method script is designed.
In the following example, a cryptographic purpose was assigned to a cryptographic module, but a key was never generated for it.

Navigate to **Key Management > Module Key Policies > Module Key Rejections**.

A list of crypto modules that rejected requests displays along with the encryption key that used in the corresponding script.

![Module Key Rejections Table](image)

**Module Key Rejections**

![Note:](image)

Note: If a different script attempts to use the same cryptographic module using the same key type, the value for **Last enforced** updates. Another row does not generate.

In this example, at 2020-02-10_15:55:17, the first module rejected a request because module1’s key is compromised. At 2020-02-10_07:24:05, the second module rejected a request because the second module’s key is suspended.

To give scripts permission to use the encryption module the next time they run, create a module access policy for script encryption. For more information, refer to **Configure script access to encrypted data**.

**Schedule mass encryption, decryption, and rekeying jobs**

Schedule encryption, decryption, and rekeying jobs to run at a time that is best for your instance.

Encryption, decryption, and rekeying jobs can be time and resource intensive, so consider scheduling at non-peak hours. Also ensure that the user scheduling the job has the appropriate access for each job.

Role required: **sn_kmf.cryptographic_manager**
Mass encryption and decryption is also available from the Encrypted Field Configurations form. See Run mass encryption or decryption for instructions.

1. Navigate to **System Security > High Security Settings > Security Jobs**.
2. Click **New**.
3. Complete the scheduling form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the encryption, decryption, or re-keying job.</td>
</tr>
<tr>
<td>Type</td>
<td>Job type:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Key Migration Context to Module</strong>: Mass migration of Encryption Context keys to Encryption Modules, including creation of Module Access Policies records for access controls on the Encryption Modules</td>
</tr>
<tr>
<td></td>
<td>• <strong>Data Migration Context to Module</strong>: Migrates data encrypted by Encryption Contexts to Encryption Modules</td>
</tr>
<tr>
<td></td>
<td>• <strong>Mass Encryption Module</strong>: Encrypts any pre-existing value in the defined column/field used in the Field Encryption Configuration</td>
</tr>
<tr>
<td></td>
<td>• <strong>Mass Decryption Module</strong>: Decrypts any pre-existing value in the defined column/field used in the Field Encryption Configuration with Single Module.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Mass Decryption Multi Module</strong>: Decrypts any pre-existing value in the defined column/field used in the Field Encryption Configuration with Multiple Module.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Module Rekeying</strong>: Re-encrypts any pre-existing value in the defined column/field used in the Field Encryption Configuration using the current active key for the module.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Migrate Attachment Context to Module</strong>: Encrypts any pre-existing attachment on the table defined in the Field Encryption Configuration. Any attachment previously encrypted with a context is re-encrypted with the module.</td>
</tr>
<tr>
<td>State</td>
<td>The initial job state is New. After the job has been executed as scheduled, the state will update accordingly</td>
</tr>
<tr>
<td>Time window start</td>
<td>Start time for the job in 24-hour format.</td>
</tr>
<tr>
<td>Time window end</td>
<td>End time for the job in 24-hour format.</td>
</tr>
<tr>
<td>Table</td>
<td>Table to be encrypted or decrypted.</td>
</tr>
<tr>
<td>Field</td>
<td>Field to be encrypted or decrypted.</td>
</tr>
<tr>
<td>Summary</td>
<td>Job status information when the job is running, has completed, or has errors.</td>
</tr>
</tbody>
</table>

**Note:** Because of system overhead, you should schedule mass encryption, decryption, and rekeying jobs to run at non-peak hours. The Now Platform runs the job between the **Time window start** and
Time window end. If the job is not complete in one processing window, it continues during the next specified processing window until all processing is complete.

4. Click **Submit**.

5. After you schedule a job, you can do the following.
   - Click **Cancel Job** to cancel a running job.
   - Click **Start** to start a job immediately.
   - Click **Update** to save any changes you make to the job schedule.
   - Click **Delete** to delete the scheduled job.

Run mass encryption or decryption
You can run mass encryption on encryption configurations. Before deleting an encrypted field configuration, run a mass decryption to decrypt previously encrypted values.

Role required: security_admin
You can also create scheduled jobs for mass encryption and decryption. See Schedule mass encryption, decryption, and rekeying jobs for instructions.

Mass encryption and decryption are available only when an encrypted field configuration uses the single cryptographic module. Mass decryption is available for both the single and multiple encryption context methods.

Note: You should run mass encryption and decryption only during non-peak hours because the operations are resource and time intensive.

1. Navigate to **System Security > Field Encryption > Encrypted Field Configurations**.
2. Open the encrypted field configuration for the field you would like to mass encrypt or decrypt.
3. Under Related Links, select an available option.
   - **Schedule Mass Decryption job**
   - **Schedule Mass Encryption job**
4. Confirm your selection in the dialog.

If running a mass encryption, all values are encrypted with the encryption context defined in the encrypted field configuration record. If running a mass decryption, only fields encrypted with an encryption context you have access to are decrypted.

Note: If you attempt to **Delete** a configuration with encrypted fields, you receive the message **Please run a Mass Decryption in every encryption context where applicable before deleting to ensure the data is not encrypted.** Press **Cancel** and run a mass decryption before deleting the configuration.

Key management actions
One of the core features of KMF is to provide the capability to manage keys, such as revoking or rotating keys. KMF properly secures sensitive data with the most up-to-date encryption materials and lifecycle operations.

The following table provides a summary of the key lifecycle operations and management actions. The cryptographic module purpose is applied to the data with the cryptographic module configuration and have no impact on data.

<table>
<thead>
<tr>
<th>Key management action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate key</td>
<td>Generates a new key for the given cryptographic module. A first generated key is set to active.</td>
</tr>
<tr>
<td>Key management action</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Rotate key</td>
<td>Deactivates the current key and generates a new one. The new module key is set to current (active).</td>
</tr>
<tr>
<td>Revoke key</td>
<td>Marks the current key and lifecycle state as revoked. The cryptographic module auto-generates a new key on new data and sets the key status to active. Revoke means that the key is no longer used for encryption. However, it can still be used for decryption. You cannot destroy a key.</td>
</tr>
<tr>
<td>Suspend key</td>
<td>Marks the current key as suspended. Manually reactivate the suspended key or revoke the suspended key to generate a new module key before using this cryptographic module again</td>
</tr>
<tr>
<td>Renew key</td>
<td>Extends the life of the current key. The Renew button becomes available under the following circumstances: • You are assigned the cryptographic manager role. • The lifecycle state is marked to either Active or Renewed. • An expiration date is set in the module lifecycle definition.</td>
</tr>
</tbody>
</table>

**View and manage keys**

Review the status of any key to determine further key action, such as when to renew, rotate, suspend, deactivate, or destroy a current key.

Role required: sn_kmf.cryptographic_manager

1. Navigate to **Key Management > Cryptographic Modules > All**.
2. Select a cryptographic module.

   The Cryptographic Module <module-name> form appears.
3. On the Module Keys tab, click the key alias to review the key status on the Lifecycle <key name> form.
4. Review the form, as all fields are read-only.

**Cryptographic Lifecycle Key fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generation date</td>
<td>Displays the date the key was generated</td>
</tr>
<tr>
<td>Activation date</td>
<td>Displays the date the key was activated</td>
</tr>
<tr>
<td>Last renewal date</td>
<td>Displays the date the key was last renewed</td>
</tr>
<tr>
<td>Last rotated date</td>
<td>Displays the date the key was last rotated</td>
</tr>
<tr>
<td>Deactivation date</td>
<td>Displays the date the key was deactivated</td>
</tr>
<tr>
<td>Destruction date</td>
<td>Displays the date the key was destroyed</td>
</tr>
<tr>
<td>Key lifecycle state</td>
<td>Displays which state the key lifecycle is in</td>
</tr>
<tr>
<td>Future activation date</td>
<td>Displays the future date of which the key activates</td>
</tr>
<tr>
<td>Future renewal date</td>
<td>Displays the future date of which the key renews</td>
</tr>
<tr>
<td>Future rotation date</td>
<td>Displays the future date of which the key rotates</td>
</tr>
</tbody>
</table>
5. To perform an action on the key, click one of the following to take effect immediately:

- **Revoke Key**: Select to deactivate the key and generate a new key. Enter the reason why you are revoking the key.
- **Rotate Key**: Select to deactivate the current key and to generate a new key in its place. The new key is listed in the Module Key table and the Key Version number increments by 1.
- **Suspend Key**: Select to deactivate the current key for an allotted time period.

**Rotate keys**

For increased security, you should rotate your keys on a pre-determined schedule. Unlike encryption contexts, KMF encryption modules support a rekey of records for re-encryption with a new key.

Role required: sn_kmf.cryptographic_manager

Encryption modules support a rekey of records for re-encryption with a new key. The following demonstrates how to manually perform a key rotation operation on a KMF cryptographic module.

1. Navigate to **Key Management > Cryptographic Modules > All**.
2. Select the cryptographic module for key rotation.
3. On the **Module Keys** tab, select the Active key.

![Module Keys Tab](image)

Select the active key
Rotate key

4. Click Rotate Key.
   The key lifecycle state changes to "Deactivated." The Last rotated date, the Deactivation date, and the Key version updates.
5. Return to Cryptographic Module > Module Keys.

Module key rotation

There is an extra module key listed in the table. The newly rotated key becomes "Active" and the previous key is "Deactivated."

Import key from web service

To upload a customer supplied key, you can import a private key using a secure web service with KMF-CLE.

Role required: sn_kmf.cryptographic_manager

1. Navigate to Key Management > Cryptographic Modules > Create New.
2. Complete the form. Be sure to select `key_import` as the **Parent crypto module**.

![Cryptographic Module Form]

**Parent crypto module:** `key_import`

See [Create a cryptographic module](#) for details.

3. Select the cryptographic module from the list.
4. Click the module from the **Crypto Specifications** related list.
5. For the Origin select **Import from web service** from the Algorithm Definition step.

**Algorithm Definition Origin**

KMF Import key endpoint access is required to complete the key import process.
6. Right-click in the header bar and select **Copy sys_id**.

7. Using an API client, such as Postman, in the request **GET** field, enter: `:16001/api/sn_kmf/key/import`
   **Params**: `cryptoSpecSysID`
8. Paste the sys_id to replace the existing **Query Params Value** for the `cryptoSpecSysID`.

![Image of API request](image_url)

- **cryptoSpecSysID value**

9. In the body, select **Binary** and attach your key file to upload.
   If prompted, select **Authentication Basic** and enter the ServiceNow crypto admin credentials.

10. Click **Send**.
    The key is uploaded to the **Module Keys** related list.
11. Return to the cryptographic module and click the Module Keys related list to view the uploaded key.

Key imported from web services
KMF Resource Exchange

Resource Exchange is a KMF feature that gives you the capability to exchange resources between instances in a secure manner.

Terminology

When using the Resource Exchange, reference the following terminology:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Exchange</td>
<td>The process to exchange resources across instances</td>
</tr>
<tr>
<td>Key Exchange (KE)</td>
<td>The process to exchange keys over instances</td>
</tr>
<tr>
<td>Key Source Instance (Key Source)</td>
<td>The instance that owns the keys</td>
</tr>
<tr>
<td>Target Instance</td>
<td>The instance that requests the keys.</td>
</tr>
</tbody>
</table>

Overview

Resource Exchange leverages KMF’s cryptographic APIs to provide confidentiality, integrity, authentication, and non-repudiation. Currently, Resource Exchange supports the Key Exchange functionality. KMF Key Exchange generates automatic key exchange requests for cryptographic modules with a column_level_encryption parent module for new instances and during upgrades when using Platform Encryption modules.

KMF Key Exchange

KMF Key Exchange is a subset function of KMF Resource Exchange. Key Exchange securely transfers encryption module keys across multiple instances.

Overview of Key Exchange

KMF Key Exchange securely transfers keys across instances, from source instance to target instance. Key Exchange supports multiple modes of operations, and is out-of-the-box automated for the System Clone case. For system cloning, the cryptographic module keys (Platform Encryption) are transferred over as part of the system clone process. Another application use case for Key Exchange is Instance Data Replication (IDR).

Supported modes

Key Exchange supports three modes on the module crypto spec level:

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic (no configuration, default behavior)</td>
<td>For System Clones, all Platform Encryption module keys are sent over automatically during the cloning process without configuration.</td>
</tr>
</tbody>
</table>
### Government Community Cloud (GCC)

ServiceNow instances in the GCC environment require a workaround to Resource Exchange that requires customer-supplied key usage. For details, contact You must upload a customer-supplied key to the target instance after cloning the source instance.

**Configure Key Exchange**

KMF Key Exchange generates automatic key exchange requests for supported cryptographic modules during the instance’s fresh installation and the upgrade. KMF manages the data encryption key locally for the instance.

Role required: sn_kmf.cryptographic_manager

KMF crypto specifications/module configuration

KMF Key Exchange uses the `com.glide.kmf.global` plugin and the `glide_encryption.auto_key_exchange.enabled` system property to manage how keys are handled during an instance clone:

- **Automatic Key Exchange**: Out-of-box property `glide_encryption.auto_key_exchange.enabled` is true by default, meaning that automatic key exchange is activated when cloning an instance. The property is cloned over to the target instance.
- Users can turn off automatic key exchange by setting the property to false.

A post-cloning script running on the target instance sends requests to the key source instance during data cloning:

- Set `glide_encryption.auto_key_exchange.enabled` to true: Sends the auto key exchange requests to the key source.
- Set `glide_encryption.auto_key_exchange.enabled` to false: The post-cloning script deletes the auto key exchange requests.

1. Navigate to **Key Management > Resource Exchange Requests > New.**

<table>
<thead>
<tr>
<th>Exchange Frequency</th>
<th>Adhoc</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Instance Sys Id</td>
<td>71235f432890cfe98742</td>
</tr>
<tr>
<td>Source Instance Host</td>
<td><a href="mailto:testnode1@testservicenow.com">testnode1@testservicenow.com</a></td>
</tr>
<tr>
<td>Crypto Specifications</td>
<td>test12345</td>
</tr>
</tbody>
</table>

**Resource Exchange Request**
2. Complete the form:

**Resource Exchange Request fields**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange Frequency</td>
<td>• <strong>Adhoc</strong>: Sends ad hoc requests from the key source instance to the target instance</td>
</tr>
<tr>
<td></td>
<td>• <strong>One Time Clone</strong>: One time clone of the keys from the source crypto specifications to the target instance</td>
</tr>
<tr>
<td></td>
<td>• <strong>Recurring Clone</strong>: Clones keys from the selected source crypto specifications to the target instance on a defined recurring basis</td>
</tr>
<tr>
<td>Source Instance Sys_id</td>
<td>Enter the system id for the source instance that hosts the keys</td>
</tr>
<tr>
<td>Source Instance Host</td>
<td>Enter the name of the host instance</td>
</tr>
<tr>
<td>Crypto Specifications</td>
<td>The keys from the crypto specification from a crypto module define the keys to clone.</td>
</tr>
</tbody>
</table>

**Note:** Click the lookup icon to browse available cryptographic specifications.
3. Click **Submit**.
   The Resource Exchange Request displays in the table. There is an entry for both the request record on the Target Instance side and also an entry in the Host Instance.

   The entry shows the status of the Request, as well as the number of keys imported to the target or exported from the host.
# Request Record (on Target Instance side)

<table>
<thead>
<tr>
<th>Status</th>
<th>Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request Approved</td>
<td>2020-10-15 15:40:38</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Target Instance Host</th>
<th>Target Instance Sys Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>localhost:6084</td>
<td>e04e75c3e9230001c8e6e8a60000000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source Instance Host</th>
<th>Source Instance Sys Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>localhost:6084</td>
<td>e04e75c3e9230001c8e6e8a60000000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Exchange Frequency</th>
<th>Enable Clone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advise</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Crypto Module</th>
<th>Imported Key Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>test1</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Crypto Spec</th>
<th>Exported Key Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>test1 AES-256</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Status Last Modified By</th>
<th>Created By</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guest</td>
<td>admin</td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Recurring Key Exchange walkthrough
This walk through shows you how to set up a recurring key exchange in your instance using KMF and Resource Exchange.

This walk through shows you how a target instance requests keys from a host instance.

Before you can perform this key exchange procedure, you must clone an instance.

1. Create a crypto module or access an existing crypto module for key exchange. Ensure that keys are generated in the crypto module. Refer to Create a cryptographic module for details.
2. Define a module access policy of type Resource Exchange for the crypto module or select an existing record from the instance. Refer to Create module access policy for details.
3. From the host instance that you cloned, navigate to Key Management > Resource Exchange Requests > New.
4. Complete the form and select Recurring Clone as the Exchange Frequency.
5. From the target instance of the clone, navigate to Key Management > Resource Exchange Requests.
6. The request from the host instance is displayed in the table.

View key exchange
The administrator approves the request and the status updates to **Request Approved** and the **Imported Key Count** is listed.

For both one-time and recurring clone requests, a module access policy of type KE automatically generates. You do not have to manually configure a policy. At clone time, this policy on source invokes to auto-approve the request (and send keys to the newly cloned target).

8. Return to the host instance.
9. View the Resource Exchange Request to show the number of exported keys.
10. View the Module Access Policy that displays the Type as **Resource Exchange**.

---

**Resource Exchange in Module Access Policy**

**Platform Encryption**

Platform Encryption utilizes the Key Management Framework (KMF) to enable you to fully customize and manage how fields and attachments are encrypted and decrypted on your instance.

Platform Encryption is the successor to Column Level Encryption (CLE) using Key Management Framework (KMF) and its full support of key management functions. Platform Encryption provides key-protection and key lifecycle management for application-level field encryption. All keys are protected with a key-wrapping hierarchy that’s ultimately rooted in FIPS 140-2-L3 Hardware Security Modules (HSM).

Platform Encryption gives you the ability to manage how supported fields are encrypted and decrypted in accordance with NIST 800-57 best practice. It also enables you to use the most updated version of field-level encryption, including integration with for proper key protection and management. A subscription is required to utilize Platform Encryption.

**Note:** Platform Encryption supports on-premise customers. It does not support Domain Separation.
Encryption overview

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Support for key management** | Fundamental to Platform Encryption is the Key Management Framework (KMF). Gain the following capabilities:  
  - Key lifecycle management  
  - Key rotation. See Rotate keys for details.  
  - Key protection and key generation with FIPS 140-2-L3 High Security Modules (HSMs)  
  - Segregation of roles and duties  
  - The secure transfer of data encryption keys between instances, such as production and non-production instances  
  - Customer Supplied Keys (CSK) with key-wrapping  
  - Non-deterministic encryption  
  - Mass encryption/decryption  
  - Auditing of key access/use  
  
  See Key Management Framework (KMF) for details. |
| **Customer-supplied key** | Support for customer supplied keys  
  One of the biggest benefits of Platform Encryption is that you can use your own keys for encryption. Administrators have the choice to use ServiceNow supplied keys or your own customer supplied keys (CSK) for encryption on the Now Platform.  
  You can also manage the key life cycle and decide when to revoke, rotate, and inactivate the keys. After you enable customer supplied keys and create a cryptographic module, you must download a token and public key (ephemeral). You use the token and public key to wrap your key and upload it to the instance. If you want to start using customer supplied keys, see Configure field encryption settings to select key type and Properties for customer supplied keys. |
| **Support for both field encryption and attachment encryption** | Both field encryption and attachment encryption utilize cryptographic modules and access policies through Encrypted Field Configurations. Attachment encryption is configured to a single cryptographic module and role. See Set encrypted field configurations for more information. |
Column Level Encryption and Platform Encryption

Platform Encryption with the Key Management Framework offers an alternative encryption solution to you compared to Column Level Encryption (CLE). See Understanding the Key Management Framework for details on how Platform Encryption with KMF compares to CLE.

See Cryptographic purpose, algorithms, and key information for encryption/decryption algorithms supported.

KMF in Platform Encryption vs. CLE (with encryption contexts)

Column Level Encryption (CLE) specifies encryption contexts for the creation of encryption keys. Contexts assign based on role to uses. These encryption contexts provide only rudimentary key management capabilities.

Platform Encryption is the successor to column level encryption using KMF and its full support of key management functions. Specifically, Platform Encryption utilizes KMF’s cryptographic modules, granting you more control of server-side encryption. KMF ensures proper data encryption key protection using key hierarchy and envelope encryption. Cryptographic modules use specifications and access policies with lifecycle management control over the key for the module, whether it’s a ServiceNow key or your own customer supplied key.

The Encrypted Field Configuration form is used in both. With Platform Encryption, you choose the type of encryption: column encryption or attachment encryption.

- In the CLE model, encryption is performed via encryption contexts. Each context is mapped to a role, which is mapped to a user.
- With Platform Encryption, your instance encrypts data through cryptographic modules that you configure. You can create an access policy for each module based on role or resource exchange. See Understanding the Key Management Framework and Cryptographic module overview for an explanation of what modules are and how they work. See Create a cryptographic module and Create module access policy for instructions.

Tip:

Once you enable Platform Encryption, you can still use Column Level Encryption (CLE) framework.

If you choose not to activate Platform Encryption, you can still use CLE. Column Level Encryption contexts permit and deny access to encrypted data based on user role. See Encryption Support for information.

API support

Platform Encryption updates the setDisplayValue() and setValue() APIs so they can insert encrypted data for encrypted fields. It also enables getDisplayValue() and getValue() to return cleartext values.

The following script illustrates these API changes when the Incident short description is encrypted:

```javascript
var gr = new GlideRecord('incident'); //creates a new incident
gr.setValue('short_description','test123'); //sets the value to test123
var sys_ID = gr.insert(); //inserts the record in the Incident table.
gs.info(gr.getValue('short_description')); //displays the unencrypted value
```

If you use getValue() to get encrypted text, your script no longer returns the ciphertext. Your scripts return the plaintext, assuming that the user has access to the cryptographic module. If the user does not have access to the cryptographic module, getValue() returns the ciphertext.
Activate Platform Encryption

You can activate the Platform Encryption plugin (com.glide.now.platform.encryption) after you purchase a subscription.

Role required: admin

The following items are installed or modified with the Platform Encryption plugin (com.glide.now.platform.encryption):

- The Encryption Support (com.glide.encryption) plugin is also activated.

**Note:** The Key Management Framework (com.glide.kmf.global) plugin is already active by default.

- The glide_encryption.cle_replatforming_with_kmf property is set to opt_in.
- The glide_encryption.set_value_support_cle.disabled property is set to false, which turns on the SetValue feature. The SetValue support enables both setDisplayValue() and setValue() APIs to support encrypted data. It also enables both getDisplayValue() and getValue() to return clear text values.
- Two scheduled jobs are enabled:
  - **autoKeyMigration**: Migrates encryption context keys to Key Management Framework (KMF) Cryptographic Module Keys.
  - **autoDataMigration**: Migrates data that you already encrypted to use the KMF Cryptographic Module key.

Administrators can modify when these scheduled jobs run, and can pause or restart them at any time.

**CAUTION:**

Once you enable Platform Encryption, you cannot roll back to the Column Level Encryption framework.

1. Navigate to **System Applications > All Available Applications > All**.
2. Find the plugin, **Platform Encryption - com.glide.now.platform.encryption** using the filter criteria and search bar.
   You can search for the plugin by its name or ID. If you cannot find a plugin, you might have to request it from ServiceNow personnel. For more information, see **Request a plugin**.
3. Click **Install**, and then in the Activate Plugin dialog box, click **Activate**.

**Note:** When domain separation and delegated admin are enabled in an instance, the administrative user must be in the global domain. Otherwise, the following error appears: Application installation is unavailable because another operation is running: Plugin Activation for <plugin name>.

Migrating to Platform Encryption

Scheduled jobs migrate your keys and encrypted data from Encryption Support to Platform Encryption.

You can review the scheduled jobs by navigating to **System Security > High Security Settings > Security Jobs**:

- **autoKeyMigration**: Migrates encryption context keys to Key Management Framework (KMF) Cryptographic Module Keys.
- **autoDataMigration**: Migrates data that you already encrypted to use the KMF Cryptographic Module key.

You can modify when these scheduled jobs run, and can pause or restart them at any time.
Verify that the encrypted field configurations are using your newly migrated module keys by navigating to System Security > Field Encryption > Encrypted Field Configurations. Look for the following items:

- The Method field is Single Module.
- The Crypto module field is populated with the name of the cryptographic module that the system automatically creates. The system adds cm in front of the name of the encryption context. You can review that module and the module access policy, both of which are active and published.

Properties for customer supplied keys

If the Platform Encryption plugin is enabled, you can use system properties to key padding, the size of the ephemeral key pair, and the key validity period of your customer supplied keys.

Platform Encryption with Key Management lets you manage the full key life cycle (rotate, revoke, and destroy) of your data encryption keys. Optionally, you can securely exchange data encryption keys generated within your environment.

Note: The properties in this topic only apply to Platform Encryption functionality. Platform Encryption is available only when the Platform Encryption (com.glide.now.platform.encryption) plugin is active and column_level_encryption is the parent crypto module. See Activate Platform Encryption for more information on obtaining Platform Encryption.

Government Community Cloud (GCC)

ServiceNow instances in the GCC environment require a workaround to Resource Exchange that requires customer-supplied key usage. For details, contact You must upload a customer-supplied key to the target instance after cloning the source instance.

Key properties

After the data encryption key is imported to the instance, a secure wrapping key protects new module keys on the instance. The wrapping key is an instance key encryption key (IKEK) generated by a hardware security module (HSM) on SafeNet KeySecure.

When you provide your own key, you must wrap it with the RSA public key. Three properties define the size, padding algorithm, and validity period of the wrapping RSA key pair:

- **glide.kmf.ephemeral_key.key_padding** controls the key padding scheme for the ephemeral key. The default is OAEP SHA256, but you can also specify SHA1.
- **glide.kmf.ephemeral_key.key_size** controls the key size of the ephemeral key pair. The default key size is 4096, but you can change it to 2048 to support a smaller key size.
- **glide.kmf.ephemeral_key.key_validity_period** defines the period for which the ephemeral key pair is valid. The default is two hours.

Continue to Wrap your customer supplied key.

Wrap your customer supplied key

If you are using customer supplied keys, wrap the private key you want to use for encryption with the downloaded public key.

Note: This procedure only applies to Platform Encryption functionality. Platform Encryption functionality is available only when the Platform Encryption (com.glide.now.platform.encryption) plugin is active and column_level_encryption is the parent crypto module. See Activate Platform Encryption for more...
information on obtaining Platform Encryption and see Create a cryptographic module for more information on selecting the parent crypto module.

- Modify optional properties that control the size, padding algorithm, and validity period of the key.
- You must have your private key (.BIN) for encryption.
- You must have a cryptographic tool to wrap your key. This example uses OpenSSL 1.1.

1. Navigate to **Key Management Framework > Cryptographic Modules > All**.
2. Select the cryptographic module that you created for the customer supplied key from the Crypto Specifications related list.
3. You will be directed to the **Key Creation** step.
4. If you have not previously downloaded the wrapping key, click the link to download the `token_publickey<id>.zip` file. Save the zip file to the same location as your key.

   **Note:** Do not rename the downloaded `token_publickey<id>` file.

5. Unzip the file to your local network.
   The zip file contains two files, an import token and a public key .PEM certificate. Wrap your private key with the public key to encrypt it.
6. Copy the name of the `token_publickey` file to your clipboard.
7. From a command line, use the copied `token_publickey` file name to open the folder of the unzipped files as a placeholder for the wrapped key.
8. Edit this script by replacing the examples with the names of your crypto files. Refer to the **Key wrapping commands** table for details:

```
"downloads user.name$ cd token_publickey_<token>
openssl pkeyutl -encrypt -pubin -inkey publickey_<keyname>.PEM
    -in <keyname.bin>
    -out wrapped_key_material -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha<128 or 256> "
```

**Key wrapping commands**

<table>
<thead>
<tr>
<th>Directions</th>
<th>Command</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open the file directory where you</td>
<td>cd</td>
<td>cd token_publickey123456789</td>
</tr>
<tr>
<td>downloaded the wrapping token</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Paste the name of the</td>
<td>openssl pkeyutl -encrypt -pubin -inkey</td>
<td>publickey_586798643ffff.PEM</td>
</tr>
<tr>
<td>publickey.PEM certificate</td>
<td>publickey_&lt;keyname&gt;.PEM</td>
<td></td>
</tr>
<tr>
<td>Paste the name of your key here</td>
<td>-in</td>
<td>mykey.bin</td>
</tr>
<tr>
<td>Enter the -out command and</td>
<td>-out wrapped_key_material -pkeyopt rsa</td>
<td>N/A</td>
</tr>
<tr>
<td>specify if the key is 128 bit or 256 bit</td>
<td>padding_mode:oaep -pkeyopt rsa_oaep_md:sha256</td>
<td></td>
</tr>
</tbody>
</table>

9. Run the command. A return displays the `token_publickey_<keynumber>`. 
10. The key will be generated and a "wrapped_key_material" file added to the directory.
11. You are ready to upload the wrapped key.

Return to Configure and upload your customer supplied key to upload your wrapped key.

Configure and upload your customer supplied key
You can use your own customer supplied key instead of using the ServiceNow system-generated keys.

**Note:** This procedure only applies to Platform Encryption functionality. Platform Encryption functionality is available only when the Platform Encryption (com.glide.now.platform.encryption) plugin is active and column_level_encryption is the parent crypto module. See Activate Platform Encryption for more information on obtaining Platform Encryption and see Create a cryptographic module for more information on selecting the parent crypto module.

Roles required: security.admin, sn_kmf.cryptographic_manager

If you are NOT supplying your own keys, you do not need to perform this procedure. To create a cryptographic module with ServiceNow keys, go to Create a cryptographic module.

**Important:** You cannot revoke a customer supplied key.

1. Navigate to System Security > Field Encryption Settings and verify that Customer Supplied Keys is selected.

   ![Field Encryption Settings](image)

   **Key source selection**

   2. Click Submit.
   3. Return to Key Management > Cryptographic Module.
4. Click **Create New**.

![Cryptographic Module form]

Create new cryptographic module

5. Complete the Cryptographic Module form as follows:

**Cryptographic Module fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module name</td>
<td>Enter a name for the module.</td>
</tr>
<tr>
<td>Crypto spec template</td>
<td>Select a cryptographic template.</td>
</tr>
<tr>
<td>Name</td>
<td>Auto-populates based on the module name.</td>
</tr>
<tr>
<td>Crypto module lifecycle state</td>
<td>Select <strong>Published</strong> to activate the crypto module.</td>
</tr>
<tr>
<td>Parent crypto module</td>
<td>Select <strong>column_level_encryption</strong>. You must select <strong>column_level_encryption</strong>; to use customer-supplied keys.</td>
</tr>
</tbody>
</table>

6. Click **Submit**.

7. Select the newly created cryptographic module from the table.

In the **Crypto Specifications** related list, click the auto-generated key alias with the AES 256 CDB algorithm. The system populates the Crypto purpose and the Algorithm for CLE automatically and jumps to the **Key Origin** stage.
8. Notice that **Upload customer supplied key** is the **Origin** and the **Key alias** is already populated.

9. Click **Next** to move to the **Key Creation** stage.

   There are two links:

   - **Download wrapping key** downloads the key in a zip file containing an import token and a public key certificate, `.PEM` file. Use the import token to verify successful key wrapping per security specification for
the instance. Use the public key certificate .PEM file to wrap your customer supplied key securely before uploading it along with the token.

- **Upload customer supplied key** opens the file browser to select the token and the encrypted key that you wrapped.

<table>
<thead>
<tr>
<th>Crypto module</th>
<th>byoktest3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key alias</td>
<td>global.byoktest3</td>
</tr>
<tr>
<td>Download wrapping key</td>
<td>token_publickey_caa896bd7ca0e010f877c0a071289326.zip</td>
</tr>
<tr>
<td>Upload customer supplied key</td>
<td>Upload customer supplied key</td>
</tr>
</tbody>
</table>

**Key creation upload links**

10. Click **Download wrapping key** to save the token. Save the token to the same destination location as the key is saved on your system. Do not rename the downloaded token.

11. Run the BYOK command on a terminal to wrap the key. For more information, refer to **Wrap your customer supplied key**.

12. Click **Upload customer supplied key**.

13. Click **Browse** to select the two files, the wrapped key and the token file.

The attachments window opens and the two files are displayed in the list.

**Wrapped key attachments upload**

Select a file to remove and re-upload, if necessary.
14. Click **OK**.

    You will be returned to the Cryptographic Module screen. A confirmation message displays for a successful upload of the customer key. The key will also be listed in the Module Keys related list.
Confirmation of key upload
Now that you have finished configuring your cryptographic module with your customer-supplied key, move on to Create module access policy.

**Encrypting fields and attachments**

After you create your cryptographic modules, create encrypted field configurations and specify whether to encrypt a field on a table or encrypt attachments. You can use ServiceNow supplied keys or your own customer supplied keys.

**Note:** This topic only applies to Platform Encryption functionality. Platform Encryption functionality is available only when the Platform Encryption (com.glide.now.platform.encryption) plugin is active and column_level_encryption is the parent crypto module. See Activate Platform Encryption for more information on obtaining Platform Encryption and see Create a cryptographic module for more information on selecting the parent crypto module.

**Encryption contexts compared to encryption modules**

In this release, Platform Encryption with encryption modules replaces Column Level Encryption (CLE) and encryption contexts.

<table>
<thead>
<tr>
<th>CLE (encryption contexts)</th>
<th>Platform Encryption (encryption modules)</th>
</tr>
</thead>
<tbody>
<tr>
<td>You can encrypt only individual attachments at the table level.</td>
<td>You can encrypt all of a table's attachments.</td>
</tr>
<tr>
<td>You assign roles to encryption contexts.</td>
<td>You establish module access policies by role or resource exchange, when Platform Encryption is active. Policies accommodate scope, domain, or script access with KMF.</td>
</tr>
<tr>
<td>You can use ServiceNow generated keys or enter a key that you generate through a certificate authority and enter into an encryption context.</td>
<td>You can either use ServiceNow generated keys or provide and manage your own customer supplied keys.</td>
</tr>
</tbody>
</table>

**How to encrypt fields**

1. Specify the key source: system-generated keys or your customer supplied keys (bring your own key) in System Security > Field Encryption Settings.

2. After you specify the key source, create a new cryptographic module or use an existing cryptographic module, access policy, and instance-level lifecycle policy. Start with Create a cryptographic module for instructions. If you use customer-supplied keys, you must follow the directions in Wrap your customer supplied key and Configure and upload your customer supplied key. You can also configure properties for these keys. See Properties for customer supplied keys.

3. Create an encrypted field configuration, which is where you specify the table on which the encryption is performed and either the column in the table or the attachments in the table to encrypt. See Set encrypted field configurations to get started.

**Set encrypted field configurations**

Configure which table columns or attachments that the system should encrypt using a pre-configured cryptographic module. These encrypted field configurations replace encryption contexts.

**Note:** This procedure only applies to Platform Encryption functionality. Platform Encryption functionality is available only when the Platform Encryption (com.glide.now.platform.encryption) plugin is active.
Role required: security_admin

Make sure you are in the correct application scope so you can see the tables in that scope.

You must have a cryptographic module and access policy already created. See Create a cryptographic module to begin.

You should have already decided whether to use ServiceNow supplied keys or your own customer supplied keys on the System Security > Field Encryption Settings form. If you are using your customer supplied key and you have not already configured settings, wrapped the key, and uploaded it to the instance, start with Wrap your customer supplied key.

1. Navigate to System Security > Field Encryption > Encrypted Field Configurations.
2. Click New.
3. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Type</td>
<td><strong>Column</strong> to encrypt a table column or <strong>Attachment</strong> to encrypt all of a table's attachments. Only users with access to the cryptographic module that you specify in this encrypted field configuration can read data in the encrypted table column or access the attachment. Types of data encrypted are: * String text * Date * Date/Time * Attachments * URL</td>
</tr>
<tr>
<td>Table</td>
<td>Table whose fields or attachments are to be encrypted.</td>
</tr>
<tr>
<td>Column</td>
<td>Column (field) to be encrypted if you selected column as the type.</td>
</tr>
<tr>
<td>Active</td>
<td>Selected if the configuration is active, unselected if the configuration is not yet in use.</td>
</tr>
<tr>
<td>Crypto module</td>
<td>The cryptographic module that the encrypted field configuration applies to.</td>
</tr>
<tr>
<td>Method</td>
<td>Select <strong>Single Module</strong> to set the field configuration across one module. Select <strong>Multiple Modules</strong> for role based access that will span across more than one cryptographic module. Attachment encryption supports <strong>Single Module</strong> only.</td>
</tr>
<tr>
<td>Algorithm Encrypted Preserving [read-only]</td>
<td>Indicates if the crypto module that you selected is already configured to support non-deterministic encryption. This means that if the same data is encrypted more than once, the encryption is different each time.</td>
</tr>
</tbody>
</table>
4. Click Submit.

Platform Encryption examples

These examples walk you through the encryption of fields and attachments using customer-supplied keys.

Column encryption walkthrough

This walkthrough shows you how to encrypt a field in your instance using Platform Encryption with the Key Management Framework. It also shows you how to use your own key.

Note: This procedure only applies to Platform Encryption functionality. Platform Encryption functionality is available only when the Platform Encryption (com.glide.now.platform.encryption) plugin is active and column_level_encryption is the parent crypto module. See Activate Platform Encryption for more information on obtaining Platform Encryption and see Create a cryptographic module for more information on selecting the parent crypto module.

Role required: sn_kmf.admin

This walkthrough starts with an instance where you have already created and uploaded your personal cryptographic key. You could use the ServiceNow key, but this example uses a customer-supplied key.

After the key has been stored in a cryptographic module, you can start configuring fields in your instance, such as salary or social security numbers that have limited access from certain users. Encrypted Field Configuration allows you to specify which authorized personnel can access sensitive data.

We show you two scenarios. One example, in this task, encrypts the Short Description field in an Incident for users who are not authorized to view the sensitive data.

Attachments can also be encrypted and only visible to users who are granted access, or visible to all users that are not restricted from viewing the data. Refer to Attachment encryption walkthrough to encrypt an attachment.

1. Make sure that Platform Encryption is enabled.
2. Create a cryptographic module with column_level_encryption as the parent module.
4. Click New.
5. Complete the form:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select <strong>Column</strong> to use your personal key.</td>
</tr>
<tr>
<td>Table</td>
<td>Select the table from where the sensitive information is stored. For this example, select Incident (incident).</td>
</tr>
<tr>
<td>Column</td>
<td>Select the column, or specific information, that represents the sensitive date to be encrypted. For this example, select Short description (short_description).</td>
</tr>
<tr>
<td>Active</td>
<td>Mark <strong>Active</strong> to be able to use the field configuration.</td>
</tr>
<tr>
<td>Algorithm Equality Preserving</td>
<td>When selecting column level encryption, this field will be automatically selected, therefore, no action is required.</td>
</tr>
<tr>
<td>Crypto module</td>
<td>Select the module that you created to use with the personal key.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Method</td>
<td>Select <strong>Single Module</strong> to use the crypto module for one module. Select <strong>Multiple Modules</strong> to apply the policies across multiple modules.</td>
</tr>
</tbody>
</table>

### Encryption field configuration example

![Encryption field configuration example](image)
6. Click **Submit**.

   Establish a Module Access Policy to assign access to the cryptographic module. Refer to Create module access policy for additional information.

7. From **Key Management** select **Module Access Policies > All**.

8. Click **New**.

9. Complete the form:

   **Module access policy fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy name</td>
<td>Enter a name for the policy, such as &quot;short description.&quot;</td>
</tr>
<tr>
<td>Crypto module</td>
<td>Select the crypto module that you created to encrypt your key.</td>
</tr>
<tr>
<td>Type</td>
<td>Select <strong>Role</strong> to grant access to the encrypted field for only those that have the assigned role.</td>
</tr>
<tr>
<td><strong>Note:</strong> You can select only <strong>Role</strong> or <strong>Resource Exchange</strong> when Platform Encryption is enabled and column_level_encryption is selected as the parent module.</td>
<td></td>
</tr>
<tr>
<td>Target Role</td>
<td>Select the role that has access to the encrypted field. For this example, select <strong>Admin</strong>.</td>
</tr>
<tr>
<td>Active</td>
<td>Select this check box to be able to use the Module Access Policy.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Result</td>
<td>Select <strong>Track</strong> to enable the access to the field for the selected role. (To restrict access to that field for the selected role, select <strong>Reject</strong> or <strong>Strict Reject</strong>.)</td>
</tr>
</tbody>
</table>

**Module access policy example**

10. Click **Submit**
11. As a KMF Admin, go to **Incident > New.**
The Short description field is visible because we just specified that the Admin role user has access, Track, to that encrypted field. Notice the lock icon under the field name indicating that the field is an encrypted field.

We will now access the Incidents module as an end user to test the encrypted field configuration.

12. Log in as a user that will be restricted from viewing the encrypted data in the configured field.

13. Access the incident number, and the data in the Short description will not be visible.

![Incident Module Screenshot](image)

**Encrypted field level data**

You have now successfully used your private key to control access to a specific field using platform encryption.

**Attachment encryption walkthrough**

This walkthrough shows you how to encrypt an attachment in your instance using column level encryption with the Key Management Framework. It also shows you how to use your own key.

**Note:** This procedure only applies to Platform Encryption functionality. Platform Encryption functionality is available only when the Platform Encryption (com.glide.now.platform.encryption) plugin is active and column_level_encryption is the parent crypto module. See Activate Platform Encryption for more information on obtaining Platform Encryption and see Create a cryptographic module for more information on selecting the parent crypto module.

Role required: kmf cryptographic manager

This walkthrough starts with an instance where you have already created and uploaded your personal cryptographic key. You could use the ServiceNow® key, but this example uses a customer-supplied key.

Upload confidential attachments in your instance and limit access from certain users. Use Encrypted Field Configurations to specify which authorized personnel can access sensitive data.
We show you how to encrypt attachments to only be visible to users who are granted access, or be visible to all users that are not restricted from viewing the data. In this example, we restrict a certain role from being able to access an attachment in the **Incidents** module.

**Note:** Although you can use multiple modules with column encryption, attachment encryption must use single modules.

1. Make sure that Platform Encryption is enabled.
2. Create a cryptographic module with column_level_encryption as the parent module.
3. Navigate to **System Security > Encrypted Field Configurations**.
4. Click **New**.
5. Complete the form:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select <strong>Attachment</strong> to use your personal key for encrypting an attachment from the selected <strong>Table</strong>. For this example, select <strong>Incident</strong>.</td>
</tr>
<tr>
<td>Table</td>
<td>Select the table to access the sensitive information. For this example, select <strong>Incident [incident]</strong>.</td>
</tr>
<tr>
<td>Active</td>
<td>Mark <strong>Active</strong> to be able to use the field configuration.</td>
</tr>
<tr>
<td>Algorithm Equality Preserving</td>
<td>When selecting column level encryption, this field is visible based on the table selected.</td>
</tr>
<tr>
<td>Crypto module</td>
<td>Select the module that you created to use with the personal key.</td>
</tr>
</tbody>
</table>
Single Module is selected, as the crypto module being used is a single module. Multiple modules are not supported for attachment encryption.

**Encrypted Field Configuration table**

6. Click **Submit**.

   Establish a Module Access Policy to assign access to the cryptographic module. Refer to Create module access policy for additional information.

7. Navigate to **Key Management > Module Access Policies > All**.

8. Click **New**.

9. Complete the form:

   **Module access policy fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy name</td>
<td>Enter a name for the policy, such as &quot;Attachment policy.&quot;</td>
</tr>
<tr>
<td>Crypto module</td>
<td>Select the crypto module that you created to encrypt your key.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Type</td>
<td>Select <strong>Role</strong> to restrict access to the encrypted field from users with the assigned role.</td>
</tr>
<tr>
<td>Target Role</td>
<td>Select the role that will not have access to the encrypted field. For this example, select <strong>itil</strong>.</td>
</tr>
<tr>
<td>Active</td>
<td>Select this check box to be able to use the Module Access Policy.</td>
</tr>
<tr>
<td>Result</td>
<td>Select <strong>Strict Reject</strong> to control the access to the attachment from the selected role. (To grant access for the selected role, select <strong>Track</strong>.)</td>
</tr>
</tbody>
</table>

**Module Access Policy form**

10. **Click Submit.**
11. As admin or as a person that created the incident, navigate to **Incidents** and add an attachment to **Activities** on the **Notes** related list.

![Attachment](image)

**Attachment available per role**

12. Log in as a user that restricted from accessing the encrypted attachment.

13. Open the incident and scroll to the **Activities**: section. The link to open the attachment is not accessible for users with the restricted role.

14. You have now successfully used your private key to control access to a specific attachment using column level encryption.
**Encryption Support**

Column Level Encryption (CLE) contexts permit and deny access to encrypted data based on user role.

Column Level Encryption (CLE) is replaced by Platform Encryption

**About Column Level Encryption support**

Implementation of column-level encryption begins with defining one or more encryption “contexts” in your instances of the Now Platform. This process includes selecting the desired encryption algorithm and providing an appropriate secret key. Access to data later encrypted using the feature is role-based, with contexts being associated with roles. Users without the correct role don’t see the field at all, or if they are assigned a role with a different context, a blank field appears. Figure 1 illustrates how role-based encryption is enabled.

![Figure 1 – Role-based encryption example](image)

Here are the results of the relationships in Figure 1:

- User 1 is a member of Role 1, which provides access to Encryption Context 1. User 1 can see the contents of Field A and Field B.
- User 2 and User 3 are members of Group 1. Group 1 is a member of Role 1, which allows everyone in Group 1 access to Encryption Context 1 and allows User 2 and User 3 to see the contents of Field A and Field B.
- User 4 is not a member of any group or role and has no access to Encryption Context 1. Not only does User 4 not have access to Field A or Field B, but User 4 doesn't even see these fields on a form. On a list view, the values would be empty.

You can implement considerably more complex role-based encryption as well.
Having access to an encrypted data field by being assigned an encryption context does not necessarily mean that a user can modify the field. Role-based access also must be implemented appropriately for that field to be accessible to users who are assigned the context via a role.

Customer encryption keys for use with column-level encryption, whether provided by a customer or randomly generated by the instance, are stored in the same unique instance database where the data encrypted by them is stored. As a further security measure, they are re-encrypted with a secondary key unique for that instance, which mitigates direct access to the encryption key for any context, either by an instance administrator or ServiceNow. Column-level encryption optionally lets you store encryption keys in your own hardware security module (HSM) or other key storage appliances or services.

The system does not have access to the user contexts necessary to decrypt data, so some actions are not possible on encrypted data. Column-level encrypted data cannot be filtered or sorted. In releases prior to Kingston, the encrypted data can't be searched, and workflows can't make use of column-level encrypted data. These capabilities, along with scheduled reporting, are executed using a system service that has no access to encrypted data and cannot be assigned the context, groups, or roles to gain access.

Pros:

- Access to encrypted data is determined by user role.
- You can choose the strength of the encryption algorithm: AES-128 or AES-256.
- You can encrypt String text, Date and Date/Time fields, attachments, and URLs.
- Encryption Support provides Equality Preserving encryption.

Cons:

- Encryption Support pre-Orlando doesn't allow you to manage your own keys. The Orlando release introduces optional key management.
- Key access requires a user session with access to the context/key and doesn't work for other back-end or system user processes.
- Key access can affect application logic and require code changes.
- Key access requires you to perform network and infrastructure maintenance.
- You can't encrypt journals.
- Encryption Support doesn't provide Order Preserving encryption or standard, non-deterministic encryption.

**Encryption methods**

Fields that use Encryption Support may include:

- New or existing Encrypted Text fields.
- String, Date, Date/Time, or URL fields included in encrypted field configuration records.

The Encrypted Field Configurations table [sys_platform_encryption_configuration] contains a record for each field encrypted with Encryption Support. This table enables a security_admin to monitor all fields in the instance that uses Encryption Support. On upgrade, encrypted field configuration records are created for all existing Encrypted Text fields. When a new Encrypted Text field is added, an encrypted field configuration record is created by default.

Encrypted field configurations can encrypt fields using one of the following methods.

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Encryption Context</td>
<td>The field is encrypted with the encryption context defined in the <strong>Encryption context</strong> field. Users who do not have the encryption context cannot view or update field values.</td>
</tr>
<tr>
<td>Method</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Multiple Encryption Contexts</td>
<td>The field is encrypted with the encryption context of the first user to enter data. If the user has two or more encryption contexts, the context defined in the encryption context selector is used. Because the encryption context is set on a per record basis, fields in a list can have different encryption contexts. However, within a single record, the field can be encrypted by only one context. When an Encrypted Text field is created, an encrypted field configuration is created with the multiple encryption contexts method. Encrypted Text fields and fields encrypted with the multiple encryption contexts method behave the same.</td>
</tr>
</tbody>
</table>

**Note:** Mass encryption is not available when using the multiple encryption contexts method.

### Access to encrypted data

A user's encryption context determines access to encrypted data. Security_admin users can grant an encryption context to a user by granting the user an associated role.

To monitor the assignment of roles, the customer or ServiceNow professional services can set up security measures. For example, an email can be sent to an appointed encryption manager whenever a role associated with an encryption context is granted to a user.

**Note:** Impersonation does not change the encryption context available to a user. Even while impersonating, you have only the encryption contexts available to you originally.

<table>
<thead>
<tr>
<th>Access level</th>
<th>Data access to a field using the single encryption context method</th>
<th>Data access to a field using the multiple encryption contexts method</th>
</tr>
</thead>
<tbody>
<tr>
<td>User with no encryption contexts</td>
<td>The form hides the encrypted field. In list view, the field appears blank and cannot be edited, even if the data in the field is decrypted.</td>
<td>The form hides the encrypted field. In list view, the field appears blank and cannot be edited, even if the data in the field is decrypted.</td>
</tr>
</tbody>
</table>
| User with one encryption context    | To use the field, the user must have access to the encryption context defined in the encrypted field configuration. If the user does not have access to the encryption context, the form hides the field. In list view, the field appears blank and cannot be edited.  
  - **If there is no data in the field:** If the user has access to the encryption context, the form shows the field (assuming UI policy does not prevent it). Users with access to the encryption context can view and update the empty field. Data entered in the field is encrypted with the encryption context defined in the encrypted field configuration.  
  - **If there is data in the field:** If the user has access to the encryption context, the user can view and edit data in the field. | The user automatically uses their encryption context with the encrypted field.  
  - **If there is no data in the field:** The form shows the field (assuming UI policy does not prevent it). Users with any encryption context can view and update the empty field. Entering data in the field causes the field to use the currently selected encryption context to encrypt the data.  
  - **If there is data in the field:** If the user has access to the encryption context used to encrypt the field, the user can view and edit the field. |
## ServiceNow Platform Administration

### Limitations

- Only the following field types can be encrypted:
  - String text
  - Date
  - Date/Time
  - Attachments
  - URL

- Because contexts are tied to roles and roles are tied to users, you do not have access to keys from non-user sessions. Anything running as a system user or a scheduled job that doesn't have a user session won't be able to access the key to encrypt or decrypt data.

- Value versus display value:
  - When you use value, you get ciphertext.
  - When you use display value, provided you have the right role, you get cleartext.

Many scripts in the application layers are scripted in such a way that they ignore this distinction and use value. The data won't be encrypted or decrypted if you don't change the scripts to use display value.

### Filtering and searching encrypted fields

When an Encrypted Text field or a field with an encrypted field configuration applied is selected as the left operand in a filter, the following operators are available:

<table>
<thead>
<tr>
<th>Access level</th>
<th>Data access to a field using the single encryption context method</th>
<th>Data access to a field using the multiple encryption contexts method</th>
</tr>
</thead>
<tbody>
<tr>
<td>User with two or more encryption contexts</td>
<td>To use the field, the user must have access to the encryption context defined in the encrypted field configuration. If the user does not have access to the encryption context, the form hides the field. In list view, the field appears blank and cannot be edited.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If there is no data in the field: If the user has access to the encryption context, the form shows the field (assuming UI policy does not prevent it). Users with access to the encryption context can view and update the empty field. Data entered in the field is encrypted with the encryption context defined in the encrypted field configuration.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If there is data in the field: If the user has access to the encryption context, the user can view and edit the field. The field always uses the original encryption context to encrypt changes to the field. This behavior prevents users with two or more encryption contexts from changing the encryption context of a field.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The user can select an encryption context from the encryption context selector in the welcome bar.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If there is no data in the field: The form shows the field (assuming UI policy does not prevent it). Users with any encryption context can view and update the empty field. Entering data in the field causes the field to use the currently selected encryption context to encrypt the data. The field always uses the original encryption context to encrypt changes to the field. This behavior prevents users with two or more encryption contexts from changing the encryption context of a field.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If there is data in the field: If the user has access to the encryption context used to encrypt the field, the user can view and edit the field. The field always uses the original encryption context to encrypt changes to the field. This behavior prevents users with multiple encryption contexts from changing the encryption context of a field.</td>
<td></td>
</tr>
</tbody>
</table>
• is
• is not
• is empty
• is not empty

For Date fields, use the date picker to specify the date:

For Date/Time fields, use the date and time picker to specify the date and time:

If a user with one or more encryption contexts filters for equality or searches for a value in a list:
• Only values encrypted with an encryption context available to the user are returned.
• The operators **is empty** and **is not empty** return all matching records. Fields encrypted with an encryption context not available to the current user appear blank.

If a user does not have any encryption contexts, no records are returned.

The **Show Matching** and **Filter Out** options are supported in lists. Only exact matches are returned or filtered out.

**Note:** Adding encrypted fields in condition filters is supported in scripts such as UI policies and business rules.
Exporting data from encrypted fields

When exporting encrypted fields in a list or form to a file format, only fields encrypted by an encryption context available to the current user appear in the exported document.

To disable exports of encrypted data from a list view, add the `glide.encryption.export_encrypted_data.allowed` system property and set the value to `false`.

Activate the Encryption Support plugin

You can activate the Encryption Support plugin (com.glide.encryption) if you have the admin role.

Role required: admin

1. Navigate to System Applications > All Available Applications > All.
2. Find the plugin using the filter criteria and search bar.
   
   You can search for the plugin by its name or ID. If you cannot find a plugin, you might have to request it from ServiceNow personnel. For more information, see Request a plugin.
3. Click Install, and then in the Activate Plugin dialog box, click Activate.

   **Note:** When domain separation and delegated admin are enabled in an instance, the administrative user must be in the global domain. Otherwise, the following error appears: Application installation is unavailable because another operation is running: Plugin Activation for <plugin name>.

Set up encryption contexts

Create an encryption context that uses an encryption key. Only users who have a role associated with the encryption context can view the data encrypted with that encryption context.

Role required: security_admin

Your instance can generate an encryption key, or you can specify your own key with a certificate authority. See your certificate authority documentation for information on creating an encryption key.

Starting with the London release, the Now Platform no longer supports creating new Triple DES keys for an Encryption Context, but continues to support previously-created Triple DES keys. Previously-created Triple DES keys are listed in the Encryption Contexts with a Type of 3DES.
1. Navigate to **System Security > Field Encryption > Encryption Contexts**.
2. Click **New**.
3. Complete the form.

### Encryption Context form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the encryption context.</td>
</tr>
</tbody>
</table>
| Encryption key  | Key used to encrypt the data. Leave blank to generate a key randomly. Based on the desired type of encryption, enter the exact number of characters:  
  - 16 characters for AES 128-bit  
  - 32 characters for AES 256-bit  
  
  **Warning:** You cannot retrieve this key from the instance. If you need access to the key, save it elsewhere before clicking **Submit**. |
| Application     | Defaults to **Global** and cannot be changed. |
| Type            | Type of encryption used to encrypt your data:  
  - **AES 128-bit**: Advanced Encryption Standard  
  - **AES 256-bit**: Advanced Encryption Standard using 256-bit encryption |

4. Click **Submit**.

The newly-created encryption key is encrypted with a key the system maintains. This key is not stored in the database. This practice prevents other users from copying the key and using it to decrypt data.

5. Navigate to **System Security > Roles** and open the role record to associate with the encryption context, or create a new role.

6. Right-click the form header and select **Configure > Form Layout** to configure the Roles form to add the **Encryption context** field.

7. Select the encryption context to associate with the role (there can be only one encryption context per role).
8. Click **Update**.

You must log out of the instance and log in again to use the encryption context.

**Add an encryption context selector**
Add an encryption context selector to the welcome banner to enable users with multiple encryption contexts to select a context when entering data.

Role required: security_admin

1. Click **System UI > UI Macros**.
2. Open the encryption_select UI macro.
3. Select the **Active** check box.
4. Click **Update**.
5. Click the gear icon in the banner frame to open the System Settings window.
6. On the **General** tab, select the **Show domain picker in header** switch.
7. Reload the page to see the choice list (if you have more than one encryption context).

The encryption context selector appears in the welcome banner only for users who have multiple roles with different encryption contexts.

![Encryption: HR](image)

**Note:** The selector appears only for users who have two or more encryption contexts to choose from. Users with either one or no encryption contexts do not see the selector.

**Encrypt an existing field**
Create an encrypted field configuration to encrypt the value of an existing String, Date, Date/Time, or URL field using Encryption Support.

Role required: security_admin

You can delete encrypted field configurations created to encrypt other field types. Make sure to run a mass decryption before deleting an encrypted field configuration.

1. Navigate to **System Security > Field Encryption > Encrypted Field Configurations**.

The Encrypted Field Configurations table [sys_platform_encryption_configuration] contains a record for each field encrypted with Encryption Support. You can create encrypted field configurations to encrypt existing String, Date, Date/Time, and URL fields.

2. Click **New**.
3. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>The table that contains the field to be encrypted.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Column</td>
<td>The field to be encrypted. Only String, Date, Date/Time, and URL fields are supported.</td>
</tr>
<tr>
<td></td>
<td>• <strong>String and URL fields</strong>: You can add a new encryption configuration to either a parent table or a child table.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Date and Date/Time fields</strong>: You can create encrypted field configurations to encrypt existing Date and Date/Time fields. You can add a new encryption configuration to a parent table only. You cannot add a new encryption configuration to a child table.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Depending on the number of records affected by the Date and Date/Time fields you are encrypting, it may take up to a few minutes to create the encryption configuration. Make sure that you create the encryption configuration for Date and Date/Time fields when transaction volume on the instance is low.</td>
</tr>
<tr>
<td>Method</td>
<td>• <strong>Single Encryption Context</strong>: Enables data to be encrypted with a single encryption context only. The field is encrypted with the encryption context defined in the <strong>Encryption context</strong> field. Users that do not have the encryption context cannot view or update field values.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Multiple Encryption Contexts</strong>: Enables data to be encrypted with more than one encryption context. The field is encrypted by the encryption context of the first user to enter data. If the user has multiple encryption contexts, the context defined in the encryption context selector is used. Because the encryption context is set on a per record basis, fields in a list can have different encryption contexts. However, within a single record, the field can be encrypted by only one context.</td>
</tr>
<tr>
<td>Encryption context</td>
<td>The encryption context for the encrypted data. Only visible when <strong>Single Encryption Context</strong> is selected in the <strong>Method</strong> field.</td>
</tr>
<tr>
<td></td>
<td>Once an encrypted field configuration is applied to a field using the single encryption context method, you cannot change the encryption context.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Mass encryption is not available when using the <strong>Multiple Encryption Contexts</strong> method.</td>
</tr>
<tr>
<td></td>
<td>After a configuration is created using the single encryption context method, you can update the record to use multiple encryption contexts. However, you cannot change a field using multiple encryption contexts to use a single encryption context.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

New values added to the encrypted field are encrypted with the corresponding encryption context. If the multiple encryption contexts method is selected in the encrypted field configuration, each record is encrypted with the context of the user that enters the data.

If using the **Single Encryption Context** method and data exists in the field that you want to encrypt, open the encrypted field configuration record and select **Run mass encryption** to encrypt existing values.
Run mass encryption or decryption
You can run mass encryption on encryption configurations. Before deleting an encrypted field configuration, run a mass decryption to decrypt previously encrypted values.

Role required: security_admin
You can also create scheduled jobs for mass encryption and decryption. See Schedule mass encryption, decryption, and rekeying jobs for instructions.

Mass encryption and decryption are available only when an encrypted field configuration uses the single cryptographic module. Mass decryption is available for both the single and multiple encryption context methods.

Note: You should run mass encryption and decryption only during non-peak hours because the operations are resource and time intensive.

1. Navigate to System Security \ Field Encryption \ Encrypted Field Configurations.
2. Open the encrypted field configuration for the field you would like to mass encrypt or decrypt.
3. Under Related Links, select an available option.
   • Schedule Mass Decryption job
   • Schedule Mass Encryption job
4. Confirm your selection in the dialog.

If running a mass encryption, all values are encrypted with the encryption context defined in the encrypted field configuration record. If running a mass decryption, only fields encrypted with an encryption context you have access to are decrypted.

Note: If you attempt to Delete a configuration with encrypted fields, you receive the message Please run a Mass Decryption in every encryption context where applicable before deleting to ensure the data is not encrypted. Press Cancel and run a mass decryption before deleting the configuration.

Encrypt an attachment
You can encrypt attachments when you attach them to records.
1. Log in as a user with at least one encryption context.
2. Navigate to a form that needs an attachment added, such as the Incident or Problem form, and click the attachment icon to open the Attachments dialog box.
3. Select the file to be attached.
   Only users with one or more encryption contexts see the Encrypt check box below the file name.
4. Select the Encrypt check box.
   Important: You must select the Encrypt check box before you upload the attachment. If you don’t, the attachment won’t be encrypted.

Users with more than one encryption context are asked to confirm the encryption context. If you select a different encryption context, the encryption context selector updates to reflect the change.
5. Close the Attachments dialog box to upload the file attachment.
Attached files are listed across the top of the form. A special icon identifies encrypted files. Pointing to the icon shows the name of the encryption context. Note that you can see only encrypted files for which you have the encryption context.
Only users with the same context used to encrypt the attachment can see the attachment in the Activity Formatter. Users without the appropriate context won't see the Activity Formatter entry associated with the encrypted attachment.

**Domain separation and Column Level Encryption Support**

Domain separation is unsupported in Column Level Encryption Support, an application that provides the ability to encrypt data in an instance. The ability to access encrypted data in a domain depends on a user's role and domain assignments. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can control several aspects of this separation, including which users can see and access data.

**Support level: No support**

- The domain field may exist on data tables but there is no business logic to manage the data.
- This level is not considered domain-separated.

For more information, see [Application support for domain separation](#).

**How domain separation works in Encryption Support**

In Encryption Support, encryption configurations and keys are defined by an encryption context. You assign an encryption context to a role or roles, and then assign roles to specific users. Encryption contexts are user-specific, so when you restrict a user to specific domains, the user can access encrypted data only in the domains to which that user has access.

Domain-specific forms and fields are supported. However, there are some restrictions:

- If an encrypted field appears on multiple forms, regardless of domain, the field is encrypted on all forms in all domains.
- **Basic** domain separation is not supported because it would allow service providers (SPs) to create and manage domain-specific encryption contexts and encryption keys across all domains.
- **Standard** domain separation does not apply to encryption.
- **Enhanced** domain separation is not supported because it would allow domain administrators to create and manage domain-specific encryption contexts and keys for their domain.

**Demonstration plugin for CLE**

The instance provides a demonstration plugin called Encryption Support - Single Context Task Encryption Demo (com.snc.task_encryption.demo) for Column Level Encryption.

The demonstration plugin is meant to illustrate how to use business rules, **UI actions**, and UI policy to support encrypted fields. The plugin enforces a limit of one security context per record. The first person to add encrypted information to a record sets the context.

You should test the demonstration plugin on a non-production instance since it modifies the Task table and adds business rules and a UI policy. After activating the plugin:

1. Create one or more encryption contexts.
2. Configure the Incident form to add the **Social security number**, **Credit card**, and **Encryption context** fields.

The plugin UI actions are:

- **Add Secure Info**: appears on records without encrypted data and allows the user to display the social security numbers and credit card fields.
• **Add Secure Info**: appears on records without encrypted data and prompts the user to select an encryption context (if the user has more than one).

• **Change Encryption**: appears on records with encrypted data and prompts the user to select an encryption context (if the user has more than one).

The plugin business rules are:

• **Form Single Encryption Context**: ensures that each form only has one security context.

• **Update on New Encrypted Attachment**: ensures that each attachment has the same security context as the parent incident.

The plugin UI policies show the encrypted fields when appropriate.

### Database encryption and full-disk encryption

ServiceNow® offers database encryption and full-disk encryption methods for customers with statutory obligations for data protection which may require at-rest protection for all data.

- Database Encryption supports all stored data to be encrypted in real time providing protection for data online and offline with no loss of functionality.
- Full disk encryption protects offline data if there is disk loss or theft.

### Database Encryption

Database Encryption enables all data to be protected with symmetric AES-256 encryption, whether the database is online or offline. From the Now Platform perspective, all data flows in decrypted. This capability is available for all supported releases.

With Database Encryption, all stored data is encrypted and individual records or tables are decrypted in memory while being accessed. New or changed data is encrypted as it is entered into a table and associated activity log files (bin, redo, undo, and error) are also encrypted.

Database Encryption is transparent to users, with no loss of functionality. When using this feature, all instances are encrypted, along with replication traffic and backups. Instance cloning is still available with a minor performance impact for using Database Encryption of up to 5%. Both new and existing instances on supported releases of the Now Platform can take advantage of database encryption.

As illustrated, ServiceNow stores and manages keys using a three-level key hierarchy:
1. A customer specific AES-256 key is created by the database engine and is used to encrypt the data.

2. A second customer specific AES-256 key is created by the database engine and is used to protect the first-level key.

3. A third AES-256 key is created by and stored within FIPS 140 validated key management appliances in the ServiceNow datacenters. This key protects the second-level key and is unique per customer instance.

The Now Platform also supports database encryption with a customer supplied switch, DBE with CCS. This is an encryption solution that encrypts all data-at-rest when not in use in the database. It uses industry standard AES encryption with no impact to functionality. The database encrypts data as it is written to the disk, and decrypts data as it is read from the disk. That means that applications always have the data in an unencrypted state to perform the necessary logic and functions without impact.

If you are using your own keys for database encryption, see Database Encryption with Customer-Controlled Switch (DBE with CCS).

**Full disk encryption**

Full disk encryption may be relevant to heavily regulated organizations, but can add significant cost to a customer’s ServiceNow deployment. Measures in place by ServiceNow to mitigate loss or theft of storage devices may also be a factor in its selection.

From the Now Platform perspective, all data flows in decrypted.

Commercial environments use full disk encryption (FDE) with FIPS 140 validated hardware or storage devices that are in the process of validation along with a ServiceNow dedicated hardware option at extra cost. FDE applies to the hardware itself, and therefore provides encryption at rest for all data stored in every instance assigned to you.
Encryption is applied to the entire storage system within the database server only, because this is the only customer data-storing component. FDE protects only against physical loss or theft of storage devices. When encrypted disk servers are powered on and providing data, the encryption provides no additional protection. For further details on selecting FDE and dedicated hardware options, contact your ServiceNow representative.

**Request database key rotation**

Rotate the database (DBE/TSE) key annually or as needed by submitting a request to support.

Role required: admin

Key rotation occurs at night within 24 hours prior to the expiration date and does not interrupt service for the instance.

**Note:** Currently, key rotation is only available in ServiceNow Commercial, GCC, France, and Singapore environments. Key rotation is supported for standard database rotation (DBE/TSE) and not on DBE with CCS.

Contact Customer Service and Support to request any of the following key rotation actions:

- Enroll to perform annual key rotation on all designated instances
- Obtain a historical report of the last three key rotations containing the following:
  - Instance name
  - Key name and version
  - Dates and times of rotation
- Schedule an early key rotation outside of the annual scheduled rotation.

**Database Encryption with Customer-Controlled Switch (DBE with CCS)**

Database Encryption with Customer-Controlled Switch is an encryption solution that encrypts all data-at-rest when not in use in the database.

**Multiple ServiceNow version support**

**Important:** Database Encryption is a paid infrastructure offering that is release agnostic. It can be applied to any supported release and to new or existing instances.

This solution uses industry standard AES encryption with no impact to functionality. The database encrypts data as it is written to the disk and decrypted by the database as it is read from the disk. That means that applications always have the data in an unencrypted state to perform the necessary logic and functions without impact.

This offering utilizes technology native to the database, often called Tablespace Encryption or Transparent Data Encryption. For more details on the technology, refer to the MariaDB website under Tablespace Encryption.

This offering requires you to create an API endpoint that would provide ServiceNow with your Key Encryption Key (KEK).

**What DBE with CCS protects against**

Database encryption addresses two different threat vectors. In each case, the data is encrypted and is thus of no use to the adversary.

- The threat of an adversary getting into the network, stealing the database files and exfiltrating them.
- The threat of an adversary getting into the datacenter and stealing the drives.
Database encryption does not provide protection at the application level. If application-level encryption is needed, Edge Encryption, Platform Encryption, or Column Level Encryption should be used. Database Encryption can be used with Edge Encryption and/or column-level encryption where higher levels of protection are needed. Database Encryption also does not protect against unauthorized users, either internal or external.

**Encryption components**

Encryption is a primary data security control. It works by scrambling data so that only authorized parties can understand information. In technical terms, it’s the process of converting plaintext to ciphertext.

Encryption requires the use of an encryption “key”–a string of characters used within an encryption algorithm for altering data so that it appears random. Like a physical key, it locks (encrypts) data so that only someone with the correct key can unlock (decrypt) it.

A policy might mandate data custodianship, where only you can access the data and ServiceNow does not have the key. This policy leaves you with two options to fully own key management responsibilities:

- **Edge (client-side) Encryption (EE):** An encrypted field of cipher text resides in the ServiceNow cloud:
  - If you don’t want to manage encryption keys, purchase Platform Encryption or use Encryption Support (Column Level Encryption). See any of the following resources:
    - Edge (client-side) Encryption (EE)
    - Platform Encryption
    - Encryption Support
  - Host your instance on premises.

**Your responsibility as a customer using DBE with CCS**

This offering requires you to create an API endpoint that provides ServiceNow with your Key Encryption Key (KEK). This endpoint is solely your responsibility and serves as the customer-end of the communications channel for transporting the key. The endpoint can include a URL of a server or a service. APIs work using requests and responses.

When the ServiceNow API gateway requests info from your endpoint, it receives a response. In this case, the KEK.

- Supplying your own customer supplied key (CSK) introduces an operational risk to the service. Until you are able to provide the original key used in the original encryption process, the cloud provider is unable to decrypt the data.
- If you lose the key, the data is permanently encrypted. Secure your key and establish Business Continuity/Disaster Recovery (BC/DR) options, should you be unable to access and furnish the key.

Regarding the end point, note the following requirements.

- ServiceNow does not set up your endpoint, nor does ServiceNow own any part of the customer API endpoint.
- There might not be any ServiceNow Professional Services available for setting up the endpoint.
• Your security administrators and engineers need API development expertise. Engage the IT/development resources or find a third-party SI to fulfill this obligation, as you have the sole responsibility for building and maintaining the API endpoint to the specs provided by ServiceNow. See the following Knowledge Base article: KB0789788.

• ServiceNow does not specify how you populate your endpoint with your key material. You are solely responsible for integration. For example, if you have an existing HSM/EKM/PKI that generates key material, you can use them to create and wrap the key to make it available to ServiceNow.

• If you are struggling with setting up the API endpoint, you should use the standard DBE option and then use Platform Encryption, which includes key management.

You can utilize a cloud service to host both the endpoint and populate the key using the AWS or Azure KMS. You can also engage a third-party SI or internal development resources.

**Frequently asked questions**

• What is the difference between ServiceNow database encryption (DBE) and database encryption with a customer-controlled switch (DBE with CCS)?

  With Standard DBE, ServiceNow writes a file alongside the database called “keystore_uri” which defines the location of the key. So the key (also called the KEK, or Key Encryption Key) is within the ServiceNow Hardware Security Module (HSM).

  With DBE with CCS, instead of using the ServiceNow internal HSM, the key (also called the KEK, or Key Encryption Key) location is on your endpoint.

• Do I need to provide the X509 certificates for TLS mutual authentication?

  In a TLS request, the client validates the server’s certificate. Mutual authentication means that the client also provides a certificate that the server validates against its own Trust Store. In the request from the gateway to the customer, the gateway does validate the “server” (customer endpoint) certificate. However, ServiceNow only requires that it is signed by a standard Certificate Authority (CA). You do not need to provide a certificate or CA for your endpoint as ServiceNow does not maintain certifications for customers.

  By requiring a standard CA, a high level of protection is still provided. If an attacker intercepts our request, they could return the wrong key, which would trigger an alert for ServiceNow.

• Can I configure the key_id or instance name types in the GET request "https://<customer.endpoint_host.com>/kek/<instance>/<key_id>?"

  No. The instance name is the actual name as your instance and must be precisely the same to validate with your endpoint. The key_id must be an integer and is treated as a version number.

• Can I use key rotation with this solution?

  Key rotation for DBE with CCS is not supported.

• Is IP address filtering necessary when the GET request is made to the endpoint?

  No. You wrap your key with a public key associated with your instance database. It is only decryptable by the corresponding private key, which only ServiceNow has.

• To reduce any security risk, can I allow only certain IP addresses access to the API exposed for the wrapper service?

  Yes, you can define certain IP addresses that access the API exposed for the wrapper service.

**Other references**

See these references for additional information about DBE with CCS:
How DBE with CCS works
Database encryption with a customer controlled switch requires you to set up an API endpoint and wrap your encryption key, which you then send to ServiceNow.

**Multiple ServiceNow version support**

**Important:** Database Encryption is a paid infrastructure offering that is release agnostic. It can be applied to any supported release and to new or existing instances.

This process is used by ServiceNow to obtain and unwrap a customer supplied key after you have successfully provisioned your encrypted instance.

This procedure explains the process in brief:

1. ServiceNow provides an X-DB-Certificate to you. That certificate represents the database of your instance for which ServiceNow needs the key.
2. You wrap your key with the ServiceNow public key.
3. ServiceNow unwraps your key with a ServiceNow private key.

The following diagram illustrates the flow:
Detailed encryption and decryption steps

The following steps detail how your endpoint and ServiceNow communicate to encrypt and decrypt the database. Familiarize yourself with these concepts:

- **DB Key Encryption Key (KEK)** is a key to encrypt other keys.
- ‘wrappedKey’ is your wrapped customer supplied key. There are actually two unique KEKs involved in ‘wrappedKey’:
  - Your customer supplied KEK.
  - The ServiceNow transport wrapping KEK, which is unique per customer database instance. Multiple databases for the same customer instance do not share a key. It is created using your DBI certificate public key.

TLS 1.2 is an encryption protocol intended to keep data secure when being transferred over a network. It must be enabled on your customer endpoint so ServiceNow can make a TLS 1.2 request.

1. You, as the customer, must set up an endpoint. The endpoint is solely your responsibility. Once your endpoint is set up, work with SNC Provision through a Hi request and send them your endpoint URL.
2. You, as the customer, must download the **X-DB-Certificate** attached to this Knowledge Base Article: [KB0789788](#) and remove the .txt extension.

You use the certificate to validate the connection between the ServiceNow CCS API Gateway and your endpoint. The public key from the certificate is also used to wrap your Key Encryption Key (KEK). The certificate contains `tse_<instance_name>`. As part of the validation, you must append `tse_` to the instance name before your endpoint can compare the certificate to the instance. This comparison verifies that the correct instance is making the request.

The certificate used for the request to the gateway is per-instance. Possession of this certificate authorizes the request of a key for that instance.

3. Populate the trust store with the X-DB-Certificate certificate.

4. Once you have requested the provisioning of your encrypted instance in Hi and supplied the endpoint to `thesnc-provision-dev` (SNC Provision), a datacenter instance sets up:
   - A key pair to authentication with the Gateway
   - An SNC Provision configuration for TSE on that instance.

5. **SNC Provision** sends the certificate and the URL of your endpoint to the **ServiceNow CCS Gateway**, which then makes a TLS 1.2 request to your endpoint. As part of the request, the **CCS Gateway** passes along the certificate as a header.

   A **GET** request is made to "https://<customer.endpoint_host.com>/kek/<instance>/<key_id>" where:
   - `<instance>` is an alpha-numeric string; for example: `my_instance123`.
   - `<key_id>` is an integer (ex. 456) that represents the version.

   with headers:
   - X-DB-Certificate: base 64 encoded X509 certificate in DER format.
   - Note: The base-64 encoding used is the "basic" encoding, not the URL-safe or filename-safe variants.

For more information on the response codes for the request, see [KB0789788](#).

6. Your endpoint validates the certificate in the request header. This validation confirms that the instance whose key is requested is one of your instances. It also verifies that it matches the certificate. Remember that the certificate contains "tse_<instance_name>" to identify your instance. The endpoint actually extracts the CN and Subject Alternative Name values from the certificate. Both items must be set to "tse_<instance>" where `<instance>` is the instance specified in the request. If these values are not set correctly, the request FAILs.

   Because the X-DB-Certificate is signed by the correct Certificate Authority, and represents the correct instance, this request is considered valid. However, certificates are not considered secret. So, to protect against requests from an unauthorized party that may have obtained a copy of the certificate, your customer key must be encrypted with the public key of the certificate. This encryption ensures that your key can only be decrypted by the customer database, which has the private key.

7. You, as the customer, must wrap your key (your KEK) using the RSA public key of the certificate that was passed to the endpoint and using PKCS1 OAEP padding. Your key must be 64 characters of hex (32 bytes hex-encoded). This wrapped key is included in the JSON response as the “wrappedKey”. Then you make this wrapped key available to the endpoint.

   **Important:** You, as the customer, are completely responsible for the wrapping of your key. For an example Java class you can use on your endpoint to wrap your customer supplied key, see the Knowledge Base Article [KB0789788](#). The certificate is also attached to that Knowledge Base Article.
8. The endpoint responds to the GET request with this JSON response:

Response:

- Content type: application/json
- JSON format:

```json
{
    "keyId": 1,
    "wrappedKey": "<customer key encrypted with RSA public key and base-64 encoded>",
    "validUntil": "<iso8601 timestamp>
}
```

The `validUntil` timestamp is the time after which ServiceNow must shut down the database on your instance. Your customer endpoint must always specify a future timestamp on each response to the periodic key poll, to signify that the database should remain running. If the `validUntil` time returned is in the past, that signifies that the database must be shut down immediately. Consider using a date calculated from today, such as seven days from today.

9. After the response is received, “wrappedKey” is sent back to the CCS Gateway. Also included in the response are these items:

- An HTTPS REST response code (200 means successful).
- JSON that includes these items:
  - Your KEK wrapped with the public key from the certificate.
  - The Key ID integer.
  - A valid Until Date (VuD).

10. The ServiceNow CCS Gateway then passes "wrappedKey" back to the original SNC Provision request. Since the key is wrapped using the DBI certificate public key, the gateway cannot see the key.

11. SNC Provision unwraps the returned KEK, stores a SHA256 hash of this KEK, then discards your customer supplied KEK.

- The hash confirms that the customer supplied KEK is valid/unchanged.
- Your customer supplied KEK, once unwrapped, unwraps the keystore key, which is stored temporarily on a tmpfs mount in memory. The service itself uses the keystore key to decrypt the keystore in-memory. When the keystore key is no longer needed, it's removed from the tmpfs mount.

**Warning:** When you as the customer decide to pull the "wrappedKey," ServiceNow looks at the Valid Until Date (VuD) that was sent back to SNC Provision via the Gateway. When the VuD passes, the database will close encrypted and the instance ceases operation.

SNC Provision continually checks for access to your KEK. If the polling for the number of allowable retries fails, the database closes encrypted and the instance ceases operation.

The keystore in memory is wrapped with the encrypted keystore key, and without access to the customer supplied KEK, the DB is encrypted and inaccessible.

Restoring the instance requires restoring the original wrappedKey to the endpoint. This procedure resets the # VuD and requires ServiceNow to rebuild the instance. This process might take several days.
DBE with CCS example GET request and response from the endpoint

In a DBE with CCS (Cascading Controlled Switch) scenario, the ServiceNow Gateway makes a GET request to your endpoint. This example illustrates the steps of the GET request and the JSON response.

Path of the GET request: /kek/csctest/1?sourceDBI=db169154.sjc201.service-now.com%3A3400

Header: X-DB-Certificate: MIIFITCCAwmgAwIBAgIEAck ... NxOpKHJ1 {truncated}

1. The endpoint extracts the instance name and version from the GET request path:
2. On the endpoint, the X-DB-Certificate is decoded and parsed.
3. The endpoint then extracts the CN and Subject Alternative Name values from the certificate. Both must be set to "tse_<instance>" where <instance> is the instance specified in the request. If these values are not set correctly, the request FAILs.
4. Your endpoint then extracts the public key from the certificate, and RSA encrypts your customer key using PKCS1 OAEP padding.
   The request is considered valid because the X-DB-Certificate is signed by the correct Certificate Authority. However, certificates are not considered secret. Therefore, your customer key must be encrypted with the public key of the certificate. The certificate helps protect against requests from an unauthorized party that may have obtained a copy of the certificate. #This procedure ensures that only the database of your instance has the key for decryption.
5. Your endpoint uses Base-64 to encode the encrypted key.
6. You determine the next validUntil date. #Use a date calculated from the current date.
7. The endpoint returns a status code 200 and a JSON body. The JSON body contains the key ID, the encrypted and encoded customer key, and the validUntil (VuD) date. The following code is an example:

```json
{
    "keyId": 1,
    "wrappedKey":"nyxyCw03mh8KPW51XPNHAVmm8R96nmKhmPIWU1NdqY6ebppBP2ecpHysgluxuS1a6v1cTbmPC7SgfCNKnSpBmGoN5jM8rIiRw0Lvz/yboU8q2I/Jw/9l7yy766e5y+rnz1Pckj8x5y9y1gUf/MUyf9B8wH51w5g/11jyGn5c99iF1x3zV29w5hOoN93NhOn5UmlhA0GMBu9Q67ZCw==",
    "validUntil": "2021-02-11T00:50:03Z"
}
```

Edge Encryption

ServiceNow® Edge Encryption™ encrypts sensitive data on your company premises before sending it over the Internet to your ServiceNow instance (encrypted in flight), where it remains encrypted at rest.

Explore
- Understanding Edge Encryption
- Edge Encryption components
- Encryption configurations and patterns
- Domain separation and Edge Encryption

Set up
- Planning for Edge Encryption
- Edge Encryption system requirements
- Edge Encryption installation
- Edge Encryption upgrades

Administer
- Key management for Edge Encryption
- Encrypt fields using encryption configurations
- Encrypt attachments using standard encryption
Understanding Edge Encryption

Edge Encryption is a network encryption system that resides on your network and that encrypts and decrypts sensitive data as it travels between your data center and the ServiceNow cloud.

What is Edge Encryption

The Edge Encryption feature is an additional cost option that provides you with the ability to control the end-to-end encryption of your data and key management. Edge Encryption uses a proxy application, provided by ServiceNow and installed by you within your own network. This proxy application tokenizes specified data patterns or encrypts string fields, Date fields, Date/Time fields, and attachment data before it is sent from your environment to your instance. The proxy application also decrypts the same data, again only within your own network, using keys stored only within your own network.

The relevant encryption keys and configuration exist only on the Edge proxy within your network and are not visible to ServiceNow. The data is encrypted from the moment it leaves your environment and is only decrypted upon retrieval. At no point is the data accessible in plaintext by ServiceNow systems or personnel.

Who uses Edge Encryption

Only a user logged into the instance through a proxy server on your network can view encrypted data in clear text. Likewise, only a security_admin user logged in to an instance through a proxy server in your network can configure and administer Edge Encryption.

Because the proxy server resides in your network, you own and manage the encryption keys, and they are never sent to the instance. As a result, ServiceNow never shows sensitive data in clear text.

In addition to the Edge proxy configuration and management of rules, you are responsible for the usual requirements of operating a server within your environment (including hosting, routing, backup, DNS configuration, etc.) to enable and support your Edge proxies.

Encryption and tokenization

Edge Encryption supports both encryption (through encryption configurations) and tokenization (through encryption patterns) as a means of protecting your sensitive information.

Encryption configurations

You can encrypt individual fields using encryption configurations. Edge Encryption supports AES 128-bit and AES 256-bit encryption keys. Edge Encryption supports standard, equality-preserving, and order-preserving encryption types.
In addition to attachments, you can encrypt the following field types:

- String
- Date
- Date/Time
- Journal
- Journal Input
- URL

If a Journal field marked for encryption is added to the activity stream, all user input to the field is encrypted in the activity stream.

**Note:** Multi-byte characters within supported field types can be encrypted.

### Encryption patterns

You can use encryption patterns to tokenize strings that match regular patterns such as social security and credit card numbers. While encryption configurations should be the primary method of encryption, use encryption patterns as a supplement to secure sensitive information found outside of encrypted fields.

**Note:** The Edge Encryption proxy server requires a MySQL database in your network only if using order preserving encryption or encryption patterns. Clear text values are stored in the proxy database in your network. For this reason, it is critical that you secure and regularly back up your proxy database. For recommendations, see Edge Encryption components.
Edge Encryption on the Now Platform

Edge Encryption acts as a gateway between your browser and your ServiceNow instance. Traffic from your browser passes through the gateway on its way to the ServiceNow instance. The gateway, in turn, is configured to encrypt outbound data that is marked for encryption. Inbound traffic is decrypted through the gateway, and the end user sees clear text in the browser. The advantage of this implementation from a security control perspective is that the encryption and key management are handled externally from ServiceNow.

Pro's and con's

As with Platform Encryption and Column Level encryption, Edge Encryption imposes some functional limitations within an instance as a result of the additional security. The local Edge proxy does, however, also provide some additional functionality relating to sorting when compared to column-level encryption.

Pros:
• Edge Encryption provides absolute control of who sees your information and prevents data breaches.
• Information remains on your proxy server and never leaves your network unencrypted.
• Information is encrypted in transit, before it even reaches the ServiceNow instance.
• You hold and manage all your own encryption keys. No one else, not even ServiceNow personnel, can access your keys.
• You can choose the strength of the encryption algorithm: AES-128 or AES-256.
• Edge Encryption includes the ability to encrypt String text, Date and Date/Time fields, attachments, URLs, and journals.
• Edge Encryption provides Standard, Equality Preserving, and Order Preserving encryption of data at rest within the database and instance.
• Encryption rules allow you to write custom scripts that tell the proxy server specifically what to encrypt and where to put that encrypted information in the instance. This is useful when the data structure doesn't exactly match the ServiceNow instance.
• Encryption patterns allow you to tokenize information such as passwords.

Cons:
• Edge Encryption requires an extra network hop through the Edge proxies cluster, and extra processing, which can add delay to traffic. The added processing delay of the Edge Encryption application is negligible compared to the network hop.
• Maintaining your own encryption keys can be complex and time-consuming.
• You can maintain a maximum of two keys, with no flexibility to define different keys for different subsets of columns/data, or for different roles, etc.
• Edge Encryption has the side effect that the server or platform can't decrypt the data to perform any manipulation of the decrypted data. As a consequence, functionality and data processing on the Now Platform may be restricted when encrypting columns with Edge Encryption.

What to know before you begin

Because encryption and tokenization change the nature of your data, Edge Encryption can affect other instance processes. Before using Edge Encryption, carefully consider the impact on your instance.

Because the proxy server is installed and maintained in your network, Edge Encryption requires network administration and management. Review the network requirements to ensure a smooth implementation.

Review the following topics to understand the impact of Edge Encryption on your instance:
• Planning for Edge Encryption
• Edge Encryption system requirements
• Sizing your Edge Encryption environment
• Calculate the order-preserving and tokenization database size
• Edge Encryption limitations
• Key management for Edge Encryption
**Edge Encryption components**

Edge Encryption is comprised of the Edge Encryption proxy server that runs on a server in your network, and the Edge Encryption plugin that must be installed on your ServiceNow instance. If using order-preserving encryption types or encryption patterns, a proxy database must also be installed in your network.

**Proxy application**

When going through the Edge Encryption proxy server, the Edge Encryption plugin allows you to specify which fields, patterns, and attachments should be encrypted. You can also manage encryption rules to encrypt specific requests and schedule mass encryption jobs.

**Proxy server**

The Edge Encryption proxy server uses encryption rules to identify in an HTTP request what, if anything, needs to be encrypted and encrypts it before forwarding the request to the instance. For decryption, the Edge Encryption proxy server looks at the HTTP responses for any encrypted data and decrypts it before sending the response back to the client. In order for this to happen, all HTTP requests and responses must go through the Edge Encryption proxy server. This includes any requests originating from a browser, as well as any SOAP or REST requests.

**Proxy database**

If using order preserving encryption or encryption patterns, your proxy servers rely on a MySQL database located in your network. All proxy servers in your network must use the same database.

The proxy database contains these tables.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>db_id</td>
<td>Unique database ID</td>
</tr>
<tr>
<td>edge_token_map</td>
<td>Encryption pattern data</td>
</tr>
<tr>
<td>token_map</td>
<td>Order-preserving encryption data</td>
</tr>
</tbody>
</table>

**Back up your proxy database**

Because encryption patterns rely on tokenization, clear text values are stored in your proxy database. If the database is lost, clear text values cannot be restored. It is critical that you maintain regular backups. To avoid data loss, back up your proxy database according to ServiceNow recommendations.

- Back up your database every 24 hours.
- Retain MySQL database binary log files for at least two days. After a backup has been restored, use the binary log to regenerate any data lost since the most recent backup. Refer to MySQL database backup best practices for your database version.
Edge Encryption clients
Edge Encryption uses three clients to inform the instance that the proxy is running, to synchronize requests between the proxy and the instance, and to forward all end user requests to the instance after any potential encryption.

<table>
<thead>
<tr>
<th>Client</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>heartbeat/keepalive client</td>
<td>In charge of sending a request to the ServiceNow instance every 5 seconds to let the instance know that this proxy is up and running. The requests drive the last_response_on field on the Edge proxy table, and as a consequence drive the state of the proxy. If your system has issues sending the requests, or if the request or request processing is delayed, the instance may mark the proxy as unresponsive, even if the other clients (including the one for user traffic) are up and running. This client also controls the online status of the proxy on the instance. The edgeencryption.proxy.keepalive.interval property controls the polling rate for this client. The default is 5 (seconds).</td>
</tr>
<tr>
<td>polling/sync client</td>
<td>In charge of various requests the proxy sends to the instance to synchronize on the Edge Encryption configuration (for example, which table, column, or attachment to encrypt, keys, jobs, rules, and tokenization patterns). The edgeencryption.config.poll.interval property controls the polling rate for this client. Warning: Do not change this setting. Changing the default setting of the proxy poll interval may result in synchronization delays when updating Edge Encryption settings on the instance.</td>
</tr>
<tr>
<td>default/user traffic client</td>
<td>For everything else, this client handles all end user requests and forwards them to the ServiceNow instance after any potential encryption. This client also handles responses from the instance, forwarding them to the end user after any potential decryption.</td>
</tr>
</tbody>
</table>

Key management for Edge Encryption
You are responsible for providing and managing the encryption keys used by Edge Encryption.

This topic refers to keys for the Edge Encryption product. If you are looking for information on the Key Management Framework, which can be used with Column Level Encryption, see Key Management Framework.

When obtaining and creating encryption keys to support the encryption types used by Edge Encryption, consider the following:

- Whether to use AES 128-bit or AES 256-bit. You must define a default AES 128-bit encryption key, even if it is not used.
- Whether to use file system, Java KeyStore, or Enterprise Key Management (EKM).
- When to rotate encryption keys.
- When and if to use a mass encryption job to re-encrypt data using the new key.

Before removing a key from the proxy configuration files and the keystore, it is critical that you decrypt all data on the instance that uses the key. You can do this by adding a new encryption key and scheduling a mass key rotation job.
Keystores

Edge Encryption supports the following types of key storage.

**File store**

Keys are stored in a file in a file system that is accessible by the Edge Encryption proxy. Encryption keys stored in a file are not encrypted, so it is your responsibility to protect these files.

**Java KeyStore**

Keys are stored in Java's JCEKS KeyStore. A Java KeyStore is protected by a password, so it is more secure than storing keys in a file in the file store. A single Java KeyStore can store multiple keys, and the keys are identified by a key alias, making it easier to manage multiple keys.

**Enterprise Key Management (EKM)**

Keys are stored and retrieved with the SafeNet KeySecure or Unbound Technology key management systems.

The Edge Encryption proxy ships with the Java JCEKS KeyStore file named `keystore.jceks` in the `keystore` directory. This keystore file contains the ServiceNow public key used to validate encryption rules signed by ServiceNow.

**Note:** If using a keystore other than the base system Java JCEKS KeyStore, you must import the ServiceNow public key into your keystore. The public key alias is `servicenow`.

In addition to the encryption keys, the Java JCEKS KeyStore is used to store the RSA key pair for digitally signing the encryption configuration and encryption rules that are stored in the instance, and the digital certificate that the Edge Encryption proxy uses to establish a secure connection with the browsers and any other clients.

SafeNet key versioning for Edge Encryption

Use SafeNet key versioning to simplify changing keys. Instead of creating a new alias for every new key, SafeNet key versioning keeps the same alias and increments the version.

You must set up key versioning in SafeNet before you can configure SafeNet key versioning on the Edge proxy server.

**Note:** Edge proxies installed before the London release support SafeNet keys, but do not support SafeNet key versioning. If you mistakenly use a versioned key on a Kingston or earlier proxy, when you upgrade to a London or later release, the London or later proxy detects this problem, and to prevent potential data loss the proxy does not start.

You must first schedule a mass key rotation job or a single key rotation job to replace the old SafeNet versioned key with a non-versioned key, and then create a new SafeNet versioned key, if needed. This new versioned key is safe to use with the London or later proxy, and you can restart the proxy.

Encryption key configuration

If using SafeNet versioned keys, the Change Default Keys section of the Encryption Key Configuration form includes new fields for the **Key version** of the default 128-bit and 256-bit keys. **Key version** fields are grayed out and cannot be edited.
For procedures, see Configure encryption keys on the instance.

**Versioned keys**

If using SafeNet versioned keys, when you navigate to Edge Encryption Configuration > Encryption Key Configuration > All Keys, versioned keys include the Key version.

A version number does not appear for the initial entries you make in the Change Default Keys section of the Encryption Key Configuration form. When the proxy server requests a key from SafeNet, the system adds a new line for the alias and adds the **Key version**.

In the above example, **AES128key** is listed three times:

- The first listing, with no **Key version** indicated, is the initial entry.
- The second listing, with 1 in the **Key version** column, is the first version of the key returned from SafeNet.
- The third listing, with 2 in the **Key version** column, is the second version of the key returned from SafeNet.
• As other versions of the key are returned from SafeNet, new lines are added to record the **Key version** now in use.

**Encryption configurations and patterns**
With Edge Encryption, you can encrypt fields and tokenize strings.

**Encryption configurations**

You can encrypt individual fields using encryption configurations. Edge Encryption supports AES 128-bit encryption keys. If the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy files are installed, Edge Encryption supports AES 256-bit encryption keys for each encryption type. Edge Encryption supports the following types of encryption configurations.

**Standard encryption**
The encrypted value of a field is different each time the field is encrypted, even when the field value remains the same. Standard encryption is the most robust form of encryption. Fields using standard encryption cannot be sorted, grouped by, or filtered on.

**Equality-preserving encryption**
The encrypted value of a field is the same when the field value remains the same. Supports equality comparisons and group by operations on a field.

**Note:** When equality-preserving encryption is selected for a field that already contains data, performing a group by action on the field may not group fields with the same value if one is encrypted and the other is not.

**Order-preserving encryption**
Uses tokens and encryption to secure data in your proxy database. Supports equality comparisons, group by operations, and the ability to sort data. The order preserving encryption type is only supported if there is a MySQL database configured for the Edge Encryption proxy server.

**Note:** When using order-preserving encryption and the proxy database is down, updates can be made to fields using order-preserving encryption. However, the sort order will not be correct when trying to sort data based on those fields. Groups also will not work as expected. When the proxy database is again operational, schedule an order token repair job to repair missing tokens.

**Encryption types**
The following encryption types are listed in decreasing security quality.

<table>
<thead>
<tr>
<th>Encryption type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard AES 256</td>
<td>Fields cannot be filtered, sorted, or compared.</td>
</tr>
<tr>
<td>Standard AES 128</td>
<td>Fields cannot be filtered, sorted, or compared.</td>
</tr>
<tr>
<td>Equality preserving AES 256</td>
<td>Fields can be filtered using equality comparisons.</td>
</tr>
<tr>
<td>Equality preserving AES 128</td>
<td>Fields can be filtered using equality comparisons.</td>
</tr>
<tr>
<td>Order preserving AES 256</td>
<td>Fields can be sorted and equality comparison filtering can be used. Requires the use of a MySQL database in your network.</td>
</tr>
</tbody>
</table>
### Encryption Patterns

You can secure sensitive data found in strings using encryption patterns. Once an encryption pattern is stored and activated, the Edge Encryption proxy server identifies strings that match the pattern in requests. Once located, the clear text string is stored in the proxy database and replaced on the instance with a token. Use encryption patterns to tokenize strings that match regular patterns such as social security and credit card numbers. While we recommend that encryption configurations be the primary method of encryption, use encryption patterns as a supplement to locate and secure sensitive information found outside of encrypted fields.

**Note:** The Edge Encryption proxy server requires a MySQL database in your network only if using order preserving encryption or encryption patterns. Clear text values are stored in the proxy database in your network. For this reason, it is critical that you secure and regularly back up your proxy database. For recommendations, see Edge Encryption components.

**Installed with Edge Encryption**

Edge Encryption installs tables to store encryption-related data, system properties to configure default behavior, and the edge_encryption role to administer Edge Encryption.

**Tables installed with Edge Encryption**

Edge Encryption adds the following tables.

- **Edge Encryption Configuration [sys_encryption_configuration]**
  - Contains encrypted fields and tables for which attachments are encrypted.

- **Edge Encryption Rule [sys_encryption_rule]**
  - Contains a record for each rule. A rule has a name, the condition when it is used, a script, and an order field.

- **Edge Encryption Invalid Insert Log [sys_edge_encryption_invalid_insert_log]**
  - Contains log messages created for attempts to save unencrypted data to an encrypted field.

- **Edge Encryption Proxy [sys_encryption_proxy]**
  - Contains information about the encryption proxy application.

- **Edge Proxy Encryption Type [sys_proxy_encryption_type]**
  - Used for enabling and disabling encryption types on the encryption form.

- **Encryption Job Execution [sys_encryption_job_execution]**
  - Supports mass encryption jobs.

- **Encryption Job Execution Chunk [sys_encryption_job_execution_chunk]**
  - Supports mass encryption jobs.

- **Scheduled Encryption Job [sysauto_encryption_job]**
  - Lists scheduled jobs for encryption, decryption, key rotation, order token repair, and database recovery.

- **Encryption Key Configuration [sys_encryption_key_configuration]**

---

<table>
<thead>
<tr>
<th>Encryption type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order preserving AES 128</td>
<td>Fields can be sorted and equality comparison filtering can be used. Requires the use of a MySQL database in your network.</td>
</tr>
</tbody>
</table>
Lists default encryption keys.

**Encryption Key [sys_encryption_key]**
Lists available keys and key attributes.

**Proxy Encryption Key [sys_encryption_proxy_key]**
Lists proxy encryption keys.

### Properties installed with Edge Encryption

Edge Encryption adds the following properties.

**Note:** To open the System Properties [sys_properties] table, enter `sys_properties.list` in the navigation filter.

- **glide.edge.pattern.disallowed.chars**
  A list of characters that are not allowed in patterns.
  - **Type:** a string of a comma-separated list of values
  - **Location:** System Properties [sys_properties] table

- **glide.edge.pattern.min.size**
  The minimum pattern size allowed. Allowing smaller patterns means finding more matches, which increases overhead.
  - **Type:** number
  - **Default value:** 5
  - **Location:** System Properties [sys_properties] table

- **sn_edge_encryption.logging.destination**
  Where messages are logged.
  - **Type:** string
  - **Default value:** file
  - **Location:** System Properties [sys_properties] table

- **sn_edge_encryption.logging.verbosity**
  The logging level to use.
  - **Type:** string
  - **Default value:** info
  - **Location:** System Properties [sys_properties] table

- **sn_edge_encryption.encryption.proxy.buildtag**
  The proxy version registered with your instance.
  - **Type:** string
  - **Location:** System Properties [sys_properties] table

- **sn_edge_encryption.cleartext.allowed**
When true, allows clear text to be saved in an encrypted field. This happens when a user is accessing the instance without going through the Edge Encryption proxy. When false, the system prevents clear text from being saved in an encrypted field.

- **Type**: Boolean
- **Default value**: false
- **Location**: System Properties [sys_properties] table

### Role installed with Edge Encryption

**edge_encryption**

Edge Encryption proxies log into the instance as a user, with a user name and password. The user must have this role assigned.

Contains roles: None

### Planning for Edge Encryption

Successful implementation of Edge Encryption requires planning and preparation.

Answer the following questions in the planning stage.

- Which fields are to be encrypted?
- Which encryption types are to be used?
- How many Edge Encryption proxies are needed? See Sizing your Edge Encryption environment for recommendations and considerations.
- If an order preserving encryption type or encryption patterns are to be used, where is the MySQL database located?
- Which key management system is to be used?

System administrators, network administrators, and security team members have different tasks to fulfill for implementing Edge Encryption.

- System administrators need the security-admin role. The system administrator needs to:
  - Download the Edge Encryption proxy application.
  - Set up an Edge Encryption user account for the proxies to use to connect to the instance. The user must be assigned the edge_encryption role.
  - Configure encryption keys, and set the default keys.
  - Configure Edge Encryption on the instance.
  - Schedule encryption jobs.
  - Monitor Edge Encryption.
  - Create and edit encryption rules.
- Your network administrator needs to:
  - Install the Edge Encryption proxy application.
  - Know the network addresses for the proxy servers and the proxy database used for order-preserving encryption and encryption patterns.
  - Install the proxy database to be used for order-preserving encryption and encryption patterns.
  - Start and stop the proxy applications.
  - Perform encryption key management.
  - Determine how to map users to encryption proxy applications. This can be done with DNS settings or routing rules, and is specific to each network.
  - Manage multiple proxy servers.
• Configure load balancer pools and settings.

• Your security administrator must determine the encryption types to be assigned to each field.

**Edge Encryption system requirements**

You can run the Edge Encryption proxy application on servers or virtual machines that run on Microsoft Windows or Linux operating systems. For optimum performance, ensure that your configuration meets these requirements.

**Java requirements**

The host machine installing or running the Edge Encryption proxy server must maintain a supported version of Java:

- Java 8 update 121 (8u121)
- Java 8 update 141 (8u141)
- Java 8 update 151 (8u151) or later

**Note:** Java 8 update 131 (8u131) is not supported.

- Java 11.0.6 or later

**Note:** Before installing the Edge Encryption proxy server, check that the `$JAVA_HOME` variable is pointing to a supported version of Java for each user that will run the proxy server. For example, if installing the proxy server as a local administrator on Windows, check that the `$JAVA_HOME` variable is pointing to the correct version of Java system-wide. If installing on Linux, check that each user that will run the proxy server has this variable correctly defined. If a supported version of Java is not found, the Edge Encryption proxy server will not run.

<table>
<thead>
<tr>
<th>Java Version</th>
<th>Enabling AES 256-bit Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java 8 update 141 (8u141) or earlier</td>
<td>Install the Java Cryptography Extension (JCE) jurisdiction policy files by copying them into the system Java home directory of each Edge Encryption proxy server host. Add these files to the <code>&lt;Java-home-directory&gt;/jre/lib/security</code> folder before performing a scheduled or manual upgrade. To install the AES 256-bit encryption policy files, see Enable AES 256-bit encryption for Java 8 update 141 (8u141) or earlier.</td>
</tr>
<tr>
<td>Java 8 update 151 (8u151) or later</td>
<td>A <code>java.security</code> file is downloaded with the update. Edit the <code>java.security</code> file to enable AES 256-bit encryption. To edit the <code>java-security</code> file, see Enable AES 256-bit encryption for Java 8 update 151 (8u151) or later. <strong>Note:</strong> If upgrading an Edge Encryption proxy server running on Windows to a new version of Java, you may need to copy the JCE policy files from your previous Java folder to the new Java folder.</td>
</tr>
</tbody>
</table>
Note: Java does not automatically allow unlimited strength keys. You must specifically enable the use of AES 256-bit encryption.

Support for OpenJDK

Starting with the Orlando release, the Now Platform supports the following versions of openJDK:

- OpenJDK version 8
- AdoptOpenJDK version 8
- OpenJDK version 11

Proxy server minimum configuration

A proxy server requires this minimum configuration:

- 4 GB of RAM per proxy server (6 GB is recommended for most deployments).

Note: The proxy server host requires at least 1 GB of RAM more than the proxy server. The proxy server host needs the extra 1 GB for operating system services. For example, if you configure a proxy server to use 4 GB of RAM, you must install at least 5 GB of RAM on the proxy server host.

Because the proxy server requires at least 4 GB of memory, 32-bit JREs and 32-bit operating systems are no longer supported starting with the London release.

- 3 or more GHz CPU (4-core CPU preferred for optimum performance).
- Multiple proxy servers behind a load balancer. The number of proxy servers you need depends on the number of application nodes, the number of simultaneous users, and the number of servers needed for failover. See Sizing your Edge Encryption environment for more information.
- Ability to run concurrently with other services, depending on the server utilization and resource availability.

Proxy server supported systems

The following systems are supported:

<table>
<thead>
<tr>
<th>Supported System</th>
<th>Description</th>
</tr>
</thead>
</table>
| Windows Server 2012, 2012-R2, and 2016 editions | • Virtual machines or physical hardware  
• 64-bit systems |
| Linux | • Virtual machines or physical hardware  
• 64-bit systems  
On 64-bit Linux systems, you must install the 32-bit GNU C library (glibc). The installation command for CentOS is `yum install glibc.i686`. |
Proxy server connection requirements

The proxy server that runs the Edge Encryption application must be able to communicate with machines in your network. Make sure that the proxy server has these network privileges:

<table>
<thead>
<tr>
<th>Network Privilege</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall access</td>
<td>Configure any firewalls between the proxy server and the client devices to allow a connection. If your network uses a DeMilitarized Zone (DMZ) to add an extra layer of security to your Local Area Network (LAN), and if your network security protocols limit port access from within the network to the DMZ, you might have to deploy a proxy server to a machine within the DMZ.</td>
</tr>
<tr>
<td>Network access</td>
<td>Configure each client to enable the proxy server to connect with it. If network security prevents you from configuring new machines that can connect to the clients, install the proxy server on an existing machine with connection privileges.</td>
</tr>
<tr>
<td>Instance access</td>
<td>Ensure that the proxy server has network access to the instance. Make sure that you configure the proxy server network to allow traffic over TCP port 443.</td>
</tr>
<tr>
<td>Network account</td>
<td>Install the proxy server with either a local or domain administrator.</td>
</tr>
</tbody>
</table>

Order-preserving and tokenization database system requirements

Order-preserving encryption and encryption patterns require that you configure an Oracle MySQL database for the Edge Encryption proxy server. Order-preserving encryption allows any comparison operation to be directly applied on encrypted data, without first decrypting the data. Encryption patterns let you replace string patterns with tokens (called tokenization) before they are sent to and stored in the database. Because of the size of the MySQL database, use a dedicated proxy server to run the order-preserving and tokenization database.

The minimum database system requirements include:

<table>
<thead>
<tr>
<th>MySQL Database</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>MySQL database versions 5.5 to 5.7</td>
</tr>
<tr>
<td>OS</td>
<td>64-bit systems</td>
</tr>
<tr>
<td>CPU</td>
<td>2 or more GHz CPU (4-core CPU preferred for optimum performance)</td>
</tr>
<tr>
<td>RAM</td>
<td>16 GB</td>
</tr>
<tr>
<td>Disk</td>
<td>Storage Area Network (SAN) or local storage (RAID 10 recommended)</td>
</tr>
<tr>
<td>Size</td>
<td>Determined by the number of potential records multiplied by the record size. See Calculate the order-preserving and tokenization database size.</td>
</tr>
</tbody>
</table>
MySQL Database | Requirement
--- | ---
Configuration | High availability cluster. If you are unsure of how to configure your MySQL server, contact MySQL for configuration information.

**Sizing your Edge Encryption environment**

Choosing the number of proxy servers for your environment is an important task. Consider the number of users, redundancy needs, and acceptable latency.

**Redundancy**

Maintain redundant proxy servers in case of hardware failure. Proxy servers should be located behind a load balancer to provide a functional path for all users if a proxy server is unreachable. At a minimum, ensure that two proxy servers are always available.

**Size**

Size refers to the number of proxy servers required to avoid additional latency that the encryption of data produces. Depending on use, you may want to reduce the amount of latency by adding additional proxy servers. For example, if regular mass encryptions are run, add additional proxy servers to handle the load, or run the mass encryptions when the user load is light. In addition, the hardware that the proxy server runs on influences performance and latency. Proxy servers running on hardware with faster CPUs, more CPUs, and more RAM have higher throughput than slower, limited systems.

The following guidelines assume that your proxy server is running on at least the minimum hardware requirements. To determine the number of proxy servers:

- Consider setting up one proxy server for every two application nodes on the instance.
- For redundancy, set up a minimum of two proxy servers behind a load balancer.
- Add an extra proxy server for every 500 simultaneous users.
- Depending on the desired redundancy, add additional proxy servers for failover.

For example, for an instance with 2,000 users, you should have at least five proxy servers behind a load balancer. This calculation includes one proxy server for every 500 users, with an extra proxy server for failover. Determine ahead of time when you will approach a threshold of 500 users and place another proxy server in the load balancer pool.

**Load balancers**

To balance requests and improve server response time, distribute proxy servers in a load balancer pool. Configure load balancers to use the "least connections" method. This method connects requests to the proxy server with the fewest active connections, preventing the overloading of a single proxy.

**CPU utilization**

Because data encryption and tokenization are CPU intensive operations, CPU spikes while encrypting data are normal and expected. When CPU utilization is over 80% for several minutes at a time, it likely means that the proxy server has too much work to do. When this happens, latency increases for the period that the CPU utilization is high. If latency persists, adding another proxy server may help decrease the latency.
Memory

The proxy server must have a minimum of 4 GB of RAM available (6 GB recommended). Set the proxy server initial and upper bound memory limits to the recommended settings.

Calculate the order-preserving and tokenization database size

If using order-preserving encryption or encryption patterns, determine the size of your MySQL database by multiplying the number of potential records by record size.

Use a dedicated machine to run the order-preserving and tokenization database. Do not run the database on the same hardware as the proxy server.

1. Determine the potential number of records that could include fields encrypted with order-preserving encryption.
   a) Multiply the number of encryption configurations using order-preserving encryption by the number of records each configuration is applied to.
   b) To allow for growth, multiply the result by three.

2. Multiply the result of step 1 by 1,536.
   1,536 is the average size of a record in bytes.

3. If using encryption patterns, perform steps 1–2 for tokenized records and add the result to the total.

The calculated value is the recommended size in bytes for your order-preserving and tokenization database.

Edge Encryption limitations

Edge Encryption impacts system functions. Carefully evaluate the impact of encrypting a field.

Field type restrictions

You can encrypt only the following field types:

- String
- Date
- Date/Time
- Journal
- Journal Input
- URL

You cannot encrypt the following field types:

- Choice fields
- Virtual fields
- Fields in system tables, except for certain fields in sys_user
- System fields in tables
- Number fields or fields associated with an auto-numbering scheme
- Any other field type not listed above

Additional restrictions:

- When a Journal field is encrypted, the Post button is disabled, even if there are multiple Journal fields and only one of those fields is encrypted.
- Encrypted fields are not available in Go to and header filter boxes.
- When encrypting fields used as an index, you can use only order-preserving and equality-preserving encryption types. Indexed fields cannot be encrypted using the standard encryption type.

For more information, see Field types.
Filtering and searching restrictions

Standard encryption
When you select a String, Date, Date/Time, or URL field with a standard encrypted field configuration as the left operand in a filter, no filtering options are available.

Equality-preserving encryption
When you select a String, Date, Date/Time, or URL field with an equality-preserving encrypted field configuration as the left operand in a filter, the following operators are available:
- is
- is not
- is empty
- is not empty

Order-preserving encryption
When you select a String field with an order-preserving encrypted field configuration as the left operand in a filter, the following operators are available, in addition to is, is not, is empty, and is not empty:
- greater than
- less than

When you select a Date or Date/Time field with an order-preserving encrypted field configuration as the left operand in a filter, the following operators are available, in addition to is, is not, is empty, and is not empty:
- after
- before
- after or on
- before or on

Date and Date/Time pickers
For Date fields, use the date picker to specify the date:

For Date/Time fields, use the date and time picker to specify the date and time:
List condition filters

The **Show Matching** and **Filter Out** options are supported in lists. Only exact matches are returned or filtered out.

**Note:** Adding encrypted fields in condition filters is supported in scripts such as UI policies and business rules.

Configuration restrictions

Restrictions and behavior of encryption configurations:

- After you add a field to the Edge Encryption Configuration table, you cannot delete the configuration record. If you no longer want a field to be encrypted, deactivate the record in the Edge Encryption Configuration table and schedule an encryption job to decrypt the data.
- If a field in a parent table is marked to be encrypted, the field is also encrypted in all inherited tables. For example, if the **Short description** field in the Task table is encrypted, then the contents of the **Short description** field in the Incident table are encrypted.
- If a field inherited from a parent table is marked to be encrypted, the field in the parent table cannot be encrypted. For example, if the **Short description** in the Incident table is marked to be encrypted, then the **Short description** in the Task table cannot be encrypted. In this example, you can encrypt the **Short description** in the Problem table.
- When a field with an encryption configuration defined is exported to any format, the output includes encrypted values even when exported through the proxy server.
- You cannot import data to a field with an encryption configuration defined.
- You cannot encrypt inherited Date and Date/Time fields. Date or Date/Time fields inherited from a parent table are not listed on the **Column** field drop-down list, and you cannot create Date or Date/Time encryption configurations for those fields.
- You can encrypt a String or URL field only from a parent table or a child table, but not both.

Instance restrictions

Impact of using Edge Encryption on the instance:
• Back-end logic cannot process encrypted data. When the instance contains encrypted data, any business rule, back-end script, or back-end feature that relies on evaluating the data in the encrypted field does not run correctly.

**Note:** Data encrypted with equality-preserving or order-preserving encryption still passes equivalence checks when compared against an identical encrypted value.

• Since email processing goes from the mail systems straight to the instance and cannot pass through the Edge proxy, data sent in or out via email cannot be encrypted or decrypted by the Edge proxy.
  • Data and attachments in inbound emails are not encrypted.
  • Data and attachments in outbound emails remain encrypted and cannot be decrypted.

• Scripts run on the server cannot change encrypted data.

• Global search is not supported. Because global search attempts to search both encrypted and clear text data, the results may not be as expected.

• Encrypted data cannot be copied and pasted into a record where the field is not encrypted.

• Depending on the type of encryption selected, the user interface functionality for the encrypted fields is reduced. For example, being able to compare, group by, sort, and search may be impacted. Generally, the stronger the encryption selected, the more functionality is reduced.

• Except for Java KeyStore, SafeNet, and Unbound Technology, no third-party software or hardware encryption key management is supported.

• Although multiple proxy servers connected to a single instance are supported, encryption proxy cluster management and monitoring are not available. Each proxy must be managed separately.

• System configurations such as workload and the number of encrypted fields can impact the performance of encrypted fields.

• The Edge Encryption proxy server can only connect to a single instance.

• If your instance uses an Oracle database and the String field you are marking to be encrypted is greater than 2925 characters, that field cannot be sorted even when order preserving encryption is selected.

• If your instance uses an Oracle database, Unicode AL32UTF8 is the only supported character set.

• Encrypted data cannot be used in reports.

### Edge Encryption installation

You can install an Edge Encryption proxy manually or using the Edge Encryption interactive installer.

### Java requirements

The host machine installing or running the Edge Encryption proxy server must maintain a supported version of Java:

• Java 8 update 121 (8u121)
• Java 8 update 141 (8u141)
• Java 8 update 151 (8u151) or later

**Note:** Java 8 update 131 (8u131) is not supported.

• Java 11.0.6 or later

**Note:** Before installing the Edge Encryption proxy server, check that the $JAVA_HOME variable is pointing to a supported version of Java for each user that will run the proxy server. For example, if installing the proxy server as a local administrator on Windows, check that the $JAVA_HOME variable is pointing to the correct version of Java system-wide. If installing on Linux, check that each user that will run the proxy server has this variable correctly defined. If a supported version of Java is not found, the Edge Encryption proxy server will not run.
Installing the proxy server

Installing Edge Encryption includes these steps.

- Install the Edge Encryption proxy application on a server in your network using the interactive installer or the manual installer.
- Generate the RSA key pair for digitally signing encryption configurations and encryption rules.
- Install the Java Cryptography Extension (JCE), if you plan to use AES 256 encryption.
- If you are using a secure SSL connection, obtain a server certificate and import it to the Java KeyStore.
- Set up your keystore and encryption key.
- If order preserving encryption types or encryption patterns are to be used, set up a MySQL database on a machine in your network.
- Set the desired properties. Properties are located in the `edgeencryption.properties` configuration file.
- Specify that a proxy server is a trusted source so that Edge Encryption can process requests coming from that proxy server.

Accessing the proxy server

Once installation is complete, point each user's browser to an Edge Encryption proxy using the URL format: `<host>:<port>`. Values are determined by the host and port properties in the `edgeencryption.properties` file.

As an example with the following values:

<table>
<thead>
<tr>
<th>Property</th>
<th>Example value</th>
</tr>
</thead>
<tbody>
<tr>
<td>edgeencryption.proxy.host</td>
<td>hostname.mycompany.com</td>
</tr>
<tr>
<td>edgeencryption.proxy.http.port</td>
<td>8081</td>
</tr>
</tbody>
</table>

A client will access the proxy server using the following address: `http://hostname.mycompany.com:8081/`.

**Note:** DNS settings and routing rules may be used. Host and port values are determined by your network administrator.

Request Edge Encryption

The Edge Encryption plugin (com.glide.edgeencryption) is available as a separate subscription.

To purchase a subscription, contact your ServiceNow account manager. The account manager can arrange to have the plugin activated on your organization's production and subproduction instances, generally within a few days.

If you don't have an account manager, decide to delay activation after purchase, or want to evaluate the product on a subproduction instance without charge, follow these steps.

Role required: none

1. Navigate to System Applications > All Available Applications > All.
2. On the All Applications page, click **Request Plugin** to open the Request form on HI.
3. On Now Support, select the redirect link to access the Now Support Service Portal Service Catalog.

4. On the form, fill in the fields.

**Activate Plugin request form**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Instance</td>
<td>Instance on which to activate the plugin.</td>
</tr>
<tr>
<td>Plugin Name</td>
<td>Name of the plugin to activate.</td>
</tr>
<tr>
<td>Specify the date and time you would like this plugin to be enabled</td>
<td>The date and time must be at least two business days from the current time.</td>
</tr>
<tr>
<td>Reason/Comments</td>
<td>Information that would be helpful for the ServiceNow personnel who are activating the plugin. For example, if you need the plugin activated at a specific time instead of during one of the default activation windows, specify that in the comments.</td>
</tr>
</tbody>
</table>

5. Click **Submit**.

**Set up an Edge Encryption user account**

The Edge Encryption proxies connect to the instance as a user to obtain and update encryption configuration information. Create a user account for this purpose and give the edge_encryption role to the user.

The Edge Encryption plugin must be installed before you can assign the role.

Role required: admin

1. On your ServiceNow instance, create a user account to be used by the Edge Encryption proxy applications.

2. Assign the edge_encryption role to the user.

**Download the Edge Encryption proxy server**

Download the Edge Encryption proxy server application from your instance, and then copy the file to each computer that is to run the Edge Encryption proxy server.

Before starting this procedure, the Edge Encryption plugin must be installed and activated on your instance.
Note: The Edge Encryption proxy is officially supported only on Oracle JRE.

Role required: security_admin

1. Navigate to Encryption Configuration > Installation & Downloads > Downloads.
2. If using the interactive installer, click Download. If manually installing the proxy server, select the OS version for your proxy server.

Note: Because the proxy server requires at least 4 GB of memory to run, 32-bit JREs and 32-bit operating systems are no longer supported starting with the Quebec release.

3. Copy the installer to each computer that is to run the Edge Encryption proxy server. If manually installing the Edge Encryption proxy server, copy the ZIP file to each computer that is to run the Edge Encryption proxy server.

After downloading the Edge Encryption installer, Install the Edge Encryption proxy server using the interactive installer. If installing manually, Install the Edge Encryption proxy server using the command line installer. Install the Edge Encryption proxy server on a Windows or Linux computer using the interactive installer.

Note: SafeNet KeySecure keystore files are not supported by the Edge Encryption installer. To use a SafeNet KeySecure keystore, Install the Edge Encryption proxy server using the command line installer.

The Edge Encryption plugin must be installed and activated on your instance before you start this procedure. Ensure that the latest version of Java 8 is installed on the machine running the Edge Encryption installer.

The latest version of Java 8 is Java SE 8u171/8u172.
- Java SE 8u171 includes important bug fixes. Oracle strongly recommends that all Java SE 8 users upgrade to this release.
- Java SE 8u172 is a patch-set update, including all of 8u171 plus additional bug fixes.

Role required:
- security_admin on your ServiceNow instance
- local or domain administrator on a Windows host
- service user with full file system access on a Linux host

After installing a new proxy server, you can run the installer again to perform tests to detect issues with an installation or modify current settings. Your options include:

- **Install New**: Install a new proxy server.
- **Verify Installation**: Perform tests to detect and fix issues in a previous installation.
- **Reinstall Existing**: Perform tests to detect and fix issues in a previous installation and view or modify existing settings.

Note: If installing the proxy server on a Linux machine on a privileged port (port 80 or 443), you must run the installer as a root user with full file system access. To restrict file system access after the proxy server is installed, you can use the SetUID feature in the proxy installer. To enable this feature, start the installer as root or sudo root. When prompted by the installer, provide the username and usergroup of an unprivileged user. The proxy server will install with file system privileges of the given user. You can skip this step to continue the default installation with root privileges.
Use the installer to install multiple proxies for your instance on multiple machines, ensuring that the following criteria apply:

- All proxies must have the same encryption keys and the same RSA key pair used to digitally sign encryption configurations and rules.
- The encryption key must be the default key configured on the instance.
- When a proxy database is set up as part of the installation, all proxies must use the same proxy database.

You may need a proxy database for equality-preserving encryption, order-preserving encryption, or tokenization. If you do not use any of these features, you do not need a proxy database.

To use NVDA, an Assistive Technology screen reader designed to read accessibility-enabled Java applications built for keyboard users, see Configure a Windows 64-bit host to use 32-bit NVDA with Java applications.

After installing the Edge Encryption proxy server, set the proxy server initial memory limit and upper bound memory limit.

Install the Edge Encryption proxy server (interactive installer)

Install the Edge Encryption proxy on a Windows or Linux computer.

1. Download the Edge Encryption proxy server installer.
2. Open the Edge Encryption proxy installer.

   **Note:** If installing on a Windows machine, you must run the installer as Administrator.

   a) To run the installer as Administrator on a Windows machine, right-click the Command Prompt and select **Run as administrator**.
   
   b) From the command line, navigate to the directory that contains the downloaded .jar file.
   
   c) Run the following command: `java -jar <file name>.jar`.

3. To install a new proxy server, select **Install New**.
   
   If a proxy is already installed, you can run the installer to:
   
   • **Verify Installation**: Perform tests to detect and fix issues in a previous installation.
   
   • **Reinstall Existing**: Perform tests to detect and fix issues in a previous installation and view or modify existing settings.
4. Configure the **Installation Location** and **Target ServiceNow Instance**.
   a) Click **Browse** to select an installation location or manually enter an installation path.
   b) Enter the URL of the target ServiceNow instance. Include the protocol and port number.
      ```
      https://example.servicenow.com:443
      ```
   c) Enter the user name and password for a user with the edge_encryption role on the target ServiceNow instance.

5. Click **Next**.

6. Configure the **Connection Settings** and **Proxy Settings**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Host</td>
<td>Fully qualified domain name of the machine on which you are installing the proxy server.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Click Detect FQDN to look up the machine's fully qualified domain name and auto-populate the Proxy Host field.</td>
</tr>
<tr>
<td></td>
<td>Along with the port, this property defines the URL used by the client to access the proxy server.</td>
</tr>
<tr>
<td>HTTP Port</td>
<td>Port on the proxy for HTTP communication.</td>
</tr>
<tr>
<td>HTTPS Port</td>
<td>Port on the proxy for HTTPS communication.</td>
</tr>
<tr>
<td>Proxy Name</td>
<td>Name of the proxy and the service. The proxy name must be unique.</td>
</tr>
<tr>
<td>Proxy Poll Interval</td>
<td>Poll interval in seconds. With the default setting, it takes 5 seconds for the proxy to learn of encryption configuration changes. Larger values cause the instance to take longer to detect proxies that have come online.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Changing the default setting of the Proxy Poll Interval can result in detection delays when a proxy comes online.</td>
</tr>
<tr>
<td>Proxy Keep-Alive Ping Interval</td>
<td>Time in seconds between pings issued by the proxy to the instance. Pings are issued periodically to verify connectivity between the proxy and the instance. The default value is 10. The minimum value is 5.</td>
</tr>
</tbody>
</table>

7. Click **Install**.
   The Edge Encryption proxy server installs. The installation may take a few minutes.

Configure CyberArk properties protection
   Optionally, configure CyberArk properties protection to securely store Edge Encryption passwords in a centralized and secure digital vault.

You must purchase and configure CyberArk AIM (Application Identity Management) before you can configure CyberArk connection parameters and protected credentials for a proxy server. As part of the installation of the AIM client, the `JavaPasswordSDK.jar` file is installed in the AIM client installation directory. The CyberArk vault is installed on an independent hardened server, and the AIM clients allow secure access to that server.

**Note:** You must install the CyberArk AIM client on every host computer where an Edge proxy is installed.
In the Edge installer, you must specify the location of the `JavaPasswordSDK.jar` file to set up the CyberArk connection to the Edge proxy. You must also enter other values you defined during the AIM client installation.

Setting up CyberArk password storage is optional. If you do not want to set up CyberArk password storage, click Skip through the CyberArk screens.

1. On the CyberArk Connection page of the Edge Encryption installer, enter the CyberArk connection parameters.

   **CyberArk connection parameters**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path to PasswordSDK.jar</td>
<td>The path to the <code>JavaPasswordSDK.jar</code> file installed on the host Windows machine during CyberArk configuration.</td>
</tr>
<tr>
<td>App ID</td>
<td>The App ID entered during CyberArk configuration.</td>
</tr>
<tr>
<td>Safe Name</td>
<td>The Safe Name entered during CyberArk configuration.</td>
</tr>
</tbody>
</table>

2. Click Next.

3. On the CyberArk Protected Credentials page of the installer, enter the credentials to be protected by CyberArk.
   - To use a single credential name for all protected passwords, select the **Apply one Credential Name to all Credentials** check box, enter the credential name, and click **Apply**.
   - Enter the credential name for one or more of the following fields. Credential names are the usernames entered for the SSH keys during CyberArk configuration.

   **CyberArk protected credentials**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edge Encryption User</td>
<td>The CyberArk credential name for an Edge Encryption user.</td>
</tr>
<tr>
<td>Signature Key Keystore</td>
<td>The CyberArk credential name for the signature key keystore.</td>
</tr>
<tr>
<td>HTTPS Cert Keystore</td>
<td>The CyberArk credential name for the HTTPS certification keystore.</td>
</tr>
<tr>
<td>Encryption Key Keystore</td>
<td>The CyberArk credential name for the encryption key keystore.</td>
</tr>
<tr>
<td>Database</td>
<td>The CyberArk credential name for the database keystore.</td>
</tr>
<tr>
<td>SafeNet HTTPS Cert Keystore</td>
<td>The CyberArk credential name for the SafeNet HTTPS certification keystore.</td>
</tr>
<tr>
<td>SafeNet Server</td>
<td>The CyberArk credential name for the SafeNet server.</td>
</tr>
<tr>
<td>Forward Proxy</td>
<td>The CyberArk credential name for the forward proxy.</td>
</tr>
</tbody>
</table>

4. Click Next.

Configure the signature key
   Configure the signature key after installing the proxy server through the Edge Encryption proxy installer.

   The signature key signs changes to configurations and properties made by the proxy server. The signature key must be an asymmetric RSA key pair in a JCEKS KeyStore.
**Note:** If installing multiple proxies, each proxy must use the same signature key.

1. On the Signature Key page of the Edge Encryption installer, select the keystore on the host machine to store the signature key.
   - **Create New Java KeyStore:** Enter the directory location, name, and password for the new keystore.
   - **Use Existing Keystore:** Enter the keystore file location and password.

2. Click **Next**.

3. Select or create a signature key.
   - **New Key:** Create a signature key for this proxy.
   - **Use Existing Key:** Use an RSA key-pair from the selected keystore.
   - **Import Existing Key:** Import an RSA key-pair from a different keystore. Browse to the keystore file, enter the password for the keystore, and select the key alias. Provide a new alias for the key.

4. Click **Next**.

**Configure the HTTPS certificate**

To enable clients to connect to the Edge Encryption proxy server using a secure SSL connection, import the HTTPS certificate to the proxy server.

The Edge Encryption proxy provides the HTTPS certificate to clients trying to connect.

1. On the HTTPS Certificate page of the Edge Encryption installer, select the keystore to store the certificate.
   - **Create New Java KeyStore:** Enter the directory location, name, and password for the new keystore.
   - **Use Existing Keystore:** Enter the keystore file location and password.

2. Click **Next**.

3. Select or import a certificate.
   - **Use Existing Certificate:** Use an existing certificate in the selected keystore.
   - **Import from File or KeyStore:** Import a certificate from a different keystore or a .cer file. Browse to the keystore or .cer file, enter the password, and select the alias. You must provide a new alias for the certificate.

4. Click **Next**.

**Configure the AES 128-bit encryption key**

After you configure the HTTPS certificate through the Edge Encryption proxy installer, configure the AES 128-bit encryption key to encrypt your data.

The encryption key is either a plain text file inside the `/keys` directory or a secret key inside a keystore. If you use a keystore for your AES 128-bit and AES 256-bit encryption keys, they must both use the same keystore.
If you are updating an SSL certificate on an Edge proxy server, see Update SSL certificate.

1. Select the encryption key location.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Store</td>
<td>Use a file to store a single encryption key. You can use an existing file in the /keys directory, or you can generate a new file. To generate a new file, enter an alias and click <strong>Generate</strong>. A file containing an encryption key is created.</td>
</tr>
</tbody>
</table>

**Note:** This choice designates both the storage location and the encryption key. If you select **File Store**, click **Next** and go to step 5.

<table>
<thead>
<tr>
<th>Create New Java KeyStore</th>
<th>Create a keystore to store the encryption key.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java KeyStore File</td>
<td>Store the encryption key in an existing Java KeyStore file.</td>
</tr>
</tbody>
</table>

2. Click **Next**.

3. Select or create the encryption key.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Key</td>
<td>Create an encryption key and alias.</td>
</tr>
</tbody>
</table>

**Note:** You must use lowercase letters and numbers for the alias name (key name, key alias), per Java KeyStore requirements. To find out more about the keytool utility, see the Java SE Documentation.

<table>
<thead>
<tr>
<th>Use Existing Key</th>
<th>Use an existing encryption key in the selected keystore.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import Existing Key</td>
<td>Import an encryption key from a different keystore.</td>
</tr>
</tbody>
</table>

4. Click **Next**.
5. Configure the key on the instance according to the requirements defined in your installer.

To configure the key on the instance, navigate to the instance and define a default key. See Configure encryption keys on the instance. Ensure that the key alias, size, and type match the requirements defined in the installer.
6. Once the key is configured on the instance, return to the installer and click **Next**.
Configure the AES 256-bit encryption key

After you configure the AES 128-bit key through the Edge proxy installer, you can optionally configure an AES 256-bit encryption key to encrypt your data.

The encryption key is either a plain text file inside the /keys directory or a secret key inside a keystore. If you use a keystore for your AES 128-bit and AES 256-bit encryption keys, both keys must use the same keystore. If you do not want to configure an AES 256-bit encryption key, click Skip to continue installing the proxy server.

If you are updating an SSL certificate on an Edge proxy server, see Update SSL certificate.

1. Select the encryption key location.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Store</td>
<td>Use a file to store a single encryption key. You can use an existing file in the /keys directory, or you can generate a new file. To generate a new file, enter an alias and click Generate. A file containing an encryption key is created.</td>
</tr>
</tbody>
</table>

   **Note:** This choice designates both the storage location and the encryption key. If you select File Store, click Next and go to step 5.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create New Java KeyStore</td>
<td>Create a keystore to store the encryption key.</td>
</tr>
<tr>
<td>Java KeyStore File</td>
<td>Store the encryption key in an existing Java KeyStore file.</td>
</tr>
</tbody>
</table>

2. Click Next.

3. Select or create the encryption key.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Key</td>
<td>Create an encryption key and alias.</td>
</tr>
</tbody>
</table>

   **Note:** You must use lowercase letters and numbers for the alias name (key name, key alias), per Java KeyStore requirements. To find out more about the keytool utility, see the Java SE Documentation.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Existing Key</td>
<td>Use an existing encryption key in the selected keystore.</td>
</tr>
<tr>
<td>Import Existing Key</td>
<td>Import an encryption key from a different keystore.</td>
</tr>
</tbody>
</table>

4. Click Next.

5. Optional: If you want to use AES 256-bit encryption, do the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java 8 update 141 or earlier</td>
<td>Install the Java Cryptography Extension (JCE) and overwrite the policy files in the Java home directory. See Enable AES 256-bit encryption for Java 8 update 141 (8u141) or earlier.</td>
</tr>
<tr>
<td>Java 8 update 151 or later</td>
<td>Edit the java.security policy file to allow the use of unlimited strength keys. See Enable AES 256-bit encryption for Java 8 update 151 (8u151) or later.</td>
</tr>
</tbody>
</table>

6. To use AES 256-bit encryption, you must also configure the AES 256-bit default encryption key on the instance by navigating to the instance and defining a default key.

   See Configure encryption keys on the instance. Ensure that the key alias, size, and type match the requirements defined in the installer.

7. After the key is configured on the instance, return to the installer and click Next.

Update SSL certificate
When updating an SSL certificate on an Edge proxy server, you must delete the old one.

Role required: admin

When updating the SSL certificate on the Edge proxy server, you must also delete the old certificate. If you don't, the old certificate (in the form of an alias in the KeyStore file) continues to be used even though the Edge proxy server is configured to use the new certificate.

1. On the Edge proxy server, list the entries in the Java KeyStore:

   ```
   keytool -list -keystore keystore.jceks -storetype jceks -storepass MY_SUPER_PASSWORD
   ```

2. Remove the old SSL certificate:

   ```
   keytool -delete -alias MY_OLD_ALIAS -keystore keystore.jceks -storetype jceks -storepass MY_SUPER_PASSWORD
   ```

3. Add the new SSL certificate into the Java KeyStore.

Configure the Edge Encryption proxy database

If using order-preserving encryption types or encryption patterns, you can optionally configure the Edge Encryption proxy database properties.

To use order-preserving encryption types or encryption patterns, a MySQL database running in your network is mandatory. This task connects the proxy to the database, but it does not install or configure the database.

**Note:** If using multiple proxy servers, all proxy servers must use the same proxy database. The values entered in the installer must be the same for all proxy servers.

1. Confirm or change the database URL. This URL is the location of the proxy database.
2. In the **Name** field, enter the name of the proxy database. The default value is *edgeencryption*.
3. Enter the username and password for accessing the proxy database.
4. Click **Next**.

Launch the Edge Encryption proxy server

After an Edge Encryption proxy is installed and configured, you can start the proxy from the installer.

1. After configuring keys on the instance and optionally configuring the proxy database, return to the Edge Encryption proxy installer and click **Launch**.
2. If an issue is detected, or to check the status of your proxy server, you can click **Check Status** to verify that the proxy is running.

A message displays the proxy status.

![Proxy status](image)

**Congratulations!**

The Edge Encryption proxy is ready to launch. If you would like to launch it now, hit the “Launch” button. Your instance, through the proxy, is available at:

https://172.16.0.1:1234002

If you encounter any errors, validate your configuration and correct as necessary. If the problem persists, contact ServiceNow support.

![Proxy status](image)

After successfully installing the Edge Encryption proxy server, **Set the proxy server initial memory limit and upper bound memory limit.**

Verify and troubleshoot the Edge Encryption proxy server installation

After your Edge Encryption proxy is installed, you can verify the installation to locate problems or start and stop the proxy.

1. Open the Edge Encryption proxy installer.
2. Select **Verify Installation.**
3. Click **Proxy Directory** and select the proxy directory.
4. **Click Run Tests.**

Test results display.

![Run Tests](image)

**Edge Encryption proxy installation tests**

- Encryptor File Test: Passed
- Connection to ServiceNow Instance Test: Passed
- ServiceNow Instance Authentication Test: Passed
- Valid Proxy Host Test: Passed
- KeyStores are JCEKS: Passed
- Open Signature Keystore Test: Passed
- Open Signature Key Test: Passed
- Signature Key Contains `servicenow` Certificate Test: Passed
- Signature Key is RSA Test: Passed
- Open HTTPS Keystore Test: Passed
- Open HTTPS Certificate Test: Passed

© 2017 ServiceNow. All rights reserved.
5. Click **Next**.

If an issue is encountered, you can move through the installer to correct the configuration. If no issues are encountered, the installer jumps to the **Launch** page. You can check the proxy status, stop the proxy, or start the proxy from the **Launch** page.

### Install the Edge Encryption proxy server using the command line installer

Manually install multiple Edge Encryption proxy servers in your network.

Roles required: security_admin on your ServiceNow instance and local administrator on the host machine.

If order preserving encryption types or encryption patterns are to be used, set up a MySQL database on a machine in your network if not already present.

**Note:** If using Unbound Technology encryption keys with Edge Encryption, install the proxy server using the command line installer on the Unbound client machine. The Edge Encryption proxy server must run on the same machine as the Unbound technology client.

First, set up a single Edge Encryption proxy server. After your first proxy server is successfully running, add additional proxy servers for one instance to ensure an optimal environment. See **Sizing your Edge Encryption environment** to determine the number of additional proxy servers needed.

**Install the Edge Encryption proxy server (command line installer)**

- Install an Edge Encryption proxy on a 64-bit Windows or Linux computer.
- Java 8 is required to run the installer.
- Install the Edge Encryption proxy server on a machine in your network using the appropriate command for your target machine. If installing the Edge Encryption proxy server on a Windows machine, you must additionally install the proxy server as a Windows service.
- When you upgrade the Edge Encryption proxy server, the system backs up the old proxy in the `backup.dist-upgrade-<timestamp>` directory under the current installation directory. The backup directory is generated during the upgrade process and stores the old proxy information.
- When you run an upgrade via the command line, a dist-upgrade.log may be generated in the directory where the command runs. The dist-upgrade.log contains logs for the upgrade process.
- In case of a failed upgrade, the system creates a `failed-backup.dist-upgrade-<timestamp>` directory. In addition, logs/wrapper.log in the original proxy directory may also contain failure information.

1. Create the installation directory.
2. Download the Edge Encryption proxy archive file to the installation directory.
3. Open the terminal and change to the installation directory.

**Note:** If installing on a Windows machine, you must start the Windows Command Prompt with administrator privileges.

4. Run this command for the target machine and change the variables according to your configuration:

```
java -jar edgeencryption-<version>-all.jar -m install -n <ProxyName> --instancehost <host> -p <InstancePort> --protocol https
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>version</td>
<td>Version number of the Edge Encryption proxy being used to perform the current operation.</td>
</tr>
<tr>
<td>-m</td>
<td>mode</td>
<td>The operation or mode to run in (install or dist-upgrade).</td>
</tr>
<tr>
<td>Option</td>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>-n</td>
<td>ProxyName</td>
<td>The name of the encryption proxy instance. Use a unique ProxyName to be able to identify specific proxy instances.</td>
</tr>
<tr>
<td>--instancehost</td>
<td>host</td>
<td>The host name of your ServiceNow instance (for example, mycompany.service-now.com).</td>
</tr>
<tr>
<td>-p</td>
<td>InstancePort</td>
<td>The port of your instance. When the protocol is https, the port is normally 443.</td>
</tr>
<tr>
<td>--protocol</td>
<td>protocol</td>
<td>The protocol used to access your ServiceNow instance (typically https).</td>
</tr>
</tbody>
</table>

**Note:** Do not copy and paste commands from the browser. Occasionally, copy/paste operations cause unexpected characters to be pasted to the target machine and results in the command being executed incorrectly. It is best to type out the command by hand using documentation as a reference.

To see the help screen, execute this command without arguments: `java -jar edgeencryption-<version>-all.jar`

5. If installing on a Windows machine, install the Edge Encryption proxy as a Windows service.
   a) Optionally change the name of the service. Open the `conf/wrapper.conf` file on the new proxy and set the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>wrapper.ntservice.name</td>
<td>Unique name of the Edge Encryption proxy service.</td>
</tr>
<tr>
<td>wrapper.ntservice/displayname</td>
<td>Edge Encryption proxy service display name.</td>
</tr>
<tr>
<td>wrapper.ntservice/description (Optional)</td>
<td>Proxy server description.</td>
</tr>
</tbody>
</table>

   If this step is not performed, the Edge Encryption proxy service is installed under the name **Edge Encryption**.

   b) Save and close the file.
   c) Open the Windows Command Prompt and `cd` to `ServerName_port/bin`.
   d) Execute `edgeencryption.bat install`.

The `ProxyName_port` directory is created in the current directory. The `edgeencryption.properties` file is updated with the host, port, and protocol values from the command line.

Create and configure the RSA key pair for the digital signature

Create an RSA key pair that the proxy server can use to create the digital signature for signing changes to the encryption properties and configuration.

To generate and validate the digital signature, an RSA key pair must be generated and stored in the JCEKS Java KeyStore and each proxy must be configured to use this key pair. Generate an encryption key pair using the keytool command.
To use the keytool utility with a proxy installed on SElinux (CentOS), you must enable loading of shared libraries from the proxy java-installation directory. To do this, run the following command as root.

```
chcon -R -t texrel_shlib_t proxy_install_dir/java/jre /lib
```

You must use the Java 1.8 version of the keytool utility. A copy of the utility can be found in `<proxy install dir>/java/jre/bin/keytool`.

1. Change to the KeyStore directory in the proxy download directory.
2. Change the default password.

   The default password is `changeme`.

   ```
   keytool -keystore keystore.jceks -storetype jceks -storepasswd -new <newpassword>
   ```

3. Create an encryption key pair.

   **Note:** Do not enter a password for the key when the keytool utility prompts for one.

   Enter this command on a single line.

   ```
   keytool -genkeypair -alias <key alias> -keyalg rsa -keystore keystore.jceks -storetype jceks -storepass <keystore password> -keysize 2048
   ```

4. Update the encryption proxy property file (`edgeencryption.properties`).
   a) Change to the `<installation directory>/conf/` directory.
   b) Open the `edgeencryption.properties` file.
   c) Enter the properties for the digital signature.

   These properties must be the same for all proxies.

5. Save and close the `edgeencryption.properties` file.

Import and configure the certificate for secure SSL connection

To use a secure SSL connection, import a server certificate and add it to the Java KeyStore.

You must obtain the server certificate before you can add it to the Java KeyStore.

1. Add a server certificate to the Java KeyStore.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you have the RSA private key in the Java Keystore and generated the certificate from that key.</td>
<td>keytool -import -alias keyname -file server.cert -storetype JCEKS -keystore keystore.jceks -storepass pwd</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>If you have a PKCS12 (.pfx) file that contains the RSA key and the</td>
<td>keytool -importkeystore -destkeystore keystore.jceks -deststoretype jceks</td>
</tr>
<tr>
<td>certificate.</td>
<td>-srckeystore &lt;PKCS12 filename&gt; -srcstoretype pkcs12</td>
</tr>
</tbody>
</table>

Make sure that the private key password is the same as the Java KeyStore password.

You can run this command to change the password.

```
keytool -keypasswd -keystore keystore.jceks -alias <key alias>
```

For testing, you can use this command to generate a self-signed certificate.

```
keytool -genkeypair -alias cert -keystore keystore.jceks -storetype jceks -keyalg rsa
```

2. Update the `edgeencryption.properties` file.
   a) Change to the `<installation directory>/conf/` directory.
   b) Open the `edgeencryption.properties` file.
   c) Enter the properties for the SSL certificate.
      
      The certificate must be the same for all proxies connecting to the same instance.

3. Save and close the `edgeencryption.properties` file.

Enable AES 256-bit encryption

256-bit encryption is more secure than 128-bit encryption, and you can optionally configure AES 256-bit encryption on the Edge Encryption proxy server host. How you enable AES 256-bit encryption depends on the Java update installed on each proxy server host.

Edge Encryption supports only AES 128-bit and AES 256-bit keys.

⚠️ **Note:** Java does not automatically allow unlimited strength keys. You must specifically enable the use of AES 256-bit encryption.

Follow the procedure for the Java version that is installed on your proxy server host:

- Enable AES 256-bit encryption for Java 8 update 141 (8u141) or earlier
- Enable AES 256-bit encryption for Java 8 update 151 (8u151) or later

Enable AES 256-bit encryption for Java 8 update 141 (8u141) or earlier

Copy the Java Cryptography Extension (JCE) jurisdiction policy files to the Java home directory of each Edge Encryption proxy server host to enable AES 256-bit encryption for Java update 141 or earlier. 256-bit keys provide greater security than 128-bit keys.

Role required: admin

Your Java home directory includes the AES 128-bit policy files by default. To enable AES 256-bit encryption, you must overwrite the Java home directory policy files with the AES 256-bit policy files. You only need to download the JCE once, but you must update every Edge Encryption proxy server host.

⚠️ **Note:** Java does not automatically allow unlimited strength keys. You must specifically enable the use of AES 256-bit encryption.

1. Download the JCE policy 8 ZIP file from Oracle.
2. Unzip the file.
3. On each proxy server host, copy the `local_policy.jar` and `US_export_policy.jar` files into the `<Java-home-directory>/jre/lib/security` folder.

Enable AES 256-bit encryption for Java 8 update 151 (8u151) or later

Edit the `java.security` policy file to enable AES 256-bit encryption for Java update 151 or later. 256-bit keys provide greater security than 128-bit keys.

Role required: admin

Perform this task in the Java home directory of each Edge Encryption proxy server host on which you want to enable AES 256-bit encryption.

**Note:** Java does not automatically allow unlimited strength keys. You must specifically enable the use of AES 256-bit encryption.

1. Navigate to `<jre_home>/lib/security/java.security` on the proxy server host, where JRE_HOME is an environment variable for both Microsoft Windows and Linux.
2. Open the `java.security` policy file and find the line for the `crypto.policy` parameter, which is commented out by default.
3. Remove the `#` character from the beginning of the `crypto.policy` line to uncomment the line, and then save the file.

**Note:** If you do not uncomment the `crypto.policy` line, Java uses `crypto.policy=limited`, which restricts encryption to AES 128-bit keys.

Set up a key store and encryption keys

Set up the key store and encryption keys used by the Edge Encryption proxy server.

1. Carefully determine the appropriate type of key store to use based on your organization's needs.

<table>
<thead>
<tr>
<th>Supported key store</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>File store</strong></td>
<td>Keys are stored in a file in a file system accessed by the Edge Encryption proxy server. Because encryption keys stored in a file are not encrypted, it is your responsibility to protect these files.</td>
</tr>
<tr>
<td><strong>Java KeyStore</strong></td>
<td>A Java KeyStore:</td>
</tr>
<tr>
<td></td>
<td>• Stores keys in a Java JCEKS KeyStore.</td>
</tr>
<tr>
<td></td>
<td>• Is password protected and more secure than storing keys in a file in the file system.</td>
</tr>
<tr>
<td></td>
<td>• Can store multiple keys. A key alias represents each key, making it easier to manage multiple keys.</td>
</tr>
</tbody>
</table>

The Edge Encryption proxy ships with the Java JCEKS KeyStore file named `keystore.jceks` in the `keystore` directory. This key store file contains the ServiceNow public key used to validate encryption rules signed by ServiceNow.
<table>
<thead>
<tr>
<th>Supported keystore</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Key Management (EKM)</td>
<td><strong>SafeNet KeySecure</strong></td>
</tr>
<tr>
<td></td>
<td>Keys are stored and retrieved with SafeNet KeySecure key management.</td>
</tr>
<tr>
<td></td>
<td>You must secure a license with Gemalto, download the libraries, and install the SafeNet KeySecure keystore on a host machine in your network before configuring the keystore on the Edge Encryption proxy server.</td>
</tr>
<tr>
<td></td>
<td><strong>Unbound Technology</strong></td>
</tr>
<tr>
<td></td>
<td>The base64-encoded wrapped encryption key is stored as text file on the Edge Encryption proxy server. The Unbound Technology implementation (previously Dyadic Security) maintains control of the wrapping key.</td>
</tr>
<tr>
<td></td>
<td>The Edge Encryption proxy server must run on the same machine as the Unbound technology client.</td>
</tr>
</tbody>
</table>

**Note:** If using a keystore other than the base system Java JCEKS KeyStore, you must import the ServiceNow public key into your keystore. The public key alias is `servicenow`.

2. Set up the keystore and encryption keys in your local network.

Set up a Java KeyStore keystore
You can use a Java KeyStore keystore to store encryption keys.

You must use the Java 1.8 version of the keytool utility. A copy of the utility can be found in `<proxy install dir>/java/jre/bin/keytool`.

The Edge Encryption proxy ships with the Java JCEKS KeyStore file named `keystore.jceks` in the `keystore` directory. This keystore file contains the ServiceNow public key used to validate encryption rules signed by ServiceNow.

1. Set up the keystore properties.
   a) Change to the `<installation directory>/conf/` directory.
   b) Open the `edgeencryption.properties` file.
   c) Enter the properties for the Java KeyStore.

2. Save and close the `edgeencryption.properties` file.

After setting up the Java KeyStore, **Create encryption keys using the Java KeyStore keytool**.

Create encryption keys using the Java KeyStore keytool
You can use the keytool shipped with the encryption proxy distribution to create AES 128-bit and AES 256-bit encryption keys.

You must use the Java 1.8 version of the keytool utility. A copy of the utility can be found in `<proxy install dir>/java/jre/bin/keytool`.

To find out more about the keytool utility, see the [Java SE Documentation](https://docs.oracle.com/javase/8/docs/technotes/tools/unix/keytool.html).
Note: The Java KeyStore requires that the alias name (key name, key alias) use lowercase letters and numbers.

1. Change to the keystore directory, `<installation directory>/keystore/`.
2. To create the encryption key, run one of the following commands.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES 128</td>
<td><code>keytool -genseckey -alias 128bitkey -keyalg aes -keysize 128 -keystore keystore.jceks -storetype jceks</code></td>
</tr>
<tr>
<td>AES 256</td>
<td><code>keytool -genseckey -alias 256bitkey -keyalg aes -keysize 256 -keystore keystore.jceks -storetype jceks</code></td>
</tr>
</tbody>
</table>

You add the alias on the instance when you assign default keys.

Note: The key password must be the same as the keystore password.

Set up a SafeNet KeySecure keystore

If you are using a SafeNet keystore, copy a set of libraries into the proxy distribution directory.

You must install and set up the SafeNet keystore before performing this step. Secure a license with Gemalto in order to download the libraries.

Note: On Linux, file paths use a forward slash (/).

1. Copy these files to the `<installation directory>/lib` directory:
   - `ingrianNAE=<version>.jar`
   - `ingrianlog4j-api=<version>.jar`
   - `ingrianlog4j-core=<version>.jar`

2. Change to the `<installation directory>/conf/` directory, and open the `edgeencryption.properties` file.
3. Enter the properties for the SafeNet keystore.

An example for a SafeNet keystore using username and password authentication.

```
edgeencryption.nae.retries = 3
edgeencryption.nae.enabled = true
edgeencryption.nae.server = url
edgeencryption.nae.port = 9000
edgeencryption.nae.protocol = ssl
edgeencryption.nae.keystore.path = keystore/safenet_truststore
edgeencryption.nae.keystore.password = password
edgeencryption.nae.user = safenet_user
```
edgeencryption.nae.password = safenet_password

An example for a SafeNet keystore using client certificate authentication. This authentication method eliminates the need to store the SafeNet server username and password in the properties file.

edgeencryption.nae.retries = 3
edgeencryption.nae.enabled = true
edgeencryption.nae.server = url
edgeencryption.nae.port = 9000
edgeencryption.nae.protocol = ssl
edgeencryption.nae.keystore.path = keystore/safenet_clientcert
edgeencryption.nae.keystore.password = password
edgeencryption.nae.client.certificate = cert_name

4. Add or create a key in the SafeNet keystore.
   You add the key name (alias) on the instance when you assign default keys.

5. Save and close the edgeencryption.properties file.

Upgrade from Kingston or lower to London or higher

If you use a SafeNet NAE server for key storage with Edge, before upgrading the proxy from Kingston or lower to London or higher, you must copy Gemalto SafeNet client ProtectApp JAR files and add new properties.

Note: On Linux, file paths use a forward slash (/).

1. Copy the following files from `<installation directory>/lib` to a directory path that is completely outside of the proxy installation directory path:
   • ingrianNAE-<version>.jar
   • ingrianlog4j-api-<version>.jar
   • ingrianlog4j-core-<version>.jar

2. On the current version (not upgraded) of the proxy, update the `<installation directory>/conf/edgeencryption.properties` file by adding the following two properties:
   • edgeencryption.ekm.provider.classname = com.snc.edgeencryption.encryption.CloudEdgeNaeKeyProvider
   • edgeencryption.thirdparty.vendor.library.path = <directory path to the directory where you copied the jar files in step 1>

3. Save the changes.

4. Proceed with the upgrade to London or higher.

Set up Unbound Technology keys

To use Unbound Technology (previously Dyadic Security) keys with Edge Encryption, store the base64-encoded wrapped encryption key as text file on the Edge Encryption proxy server and provide the wrapping key key alias. The Unbound Technology implementation maintains control of the wrapping key.

Role required: security_admin

In your Unbound Technology implementation, identify both the wrapping key and the wrapped key. Use the RSA/ECB/OAEPTWTHSHIA-256ANDMGF1PADDING algorithm for wrapping and padding. Export the wrapped key in base64-encoded text format. Save the file using the key alias as the name with no file extension.
Note: If using Unbound Technology encryption keys with Edge Encryption, install the proxy server using the command line installer on the Unbound client machine. The Edge Encryption proxy server must run on the same machine as the Unbound technology client.

1. Add the wrapped encryption key in base64-encoded text format to the `<proxy-installation-directory>/keys` directory. The name of the file must be the key alias with no file extension.

2. Update the `edgeencryption.properties` file.
   a) Open the `edgeencryption.properties` file.
   b) Enter the File store properties. Set the value of `edgeencryption.keyfile.directory` to `keys`. This property directs the proxy server to look for the encryption key in the `<Java-home-directory>/keys` directory.
   c) Uncomment the properties for the Dyadic provider configuration. Set the value of `edgeencryption.ekm.provider.rsa.wrapping.key.alias` to the wrapping key alias in your Unbound implementation.
   d) Save and close the file.

Add the encryption key alias to the instance. The encryption key alias is the file name of the wrapped encryption key added to the `<proxy-installation-directory>/keys` directory. For example, if the file in the directory is named `myunboundkey`, add this name to the `key alias` field. See Configure encryption keys on the instance.

Create an encryption key stored in a file

You can use a simple text file as a keystore. Each file holds a single encryption key.

Note: The name of the key file must match the key alias specified in the encryption keys table in the instance. See Configure encryption keys on the instance.

1. Create a file in the `/keys` folder of the proxy server installation directory.

2. Add the encryption key to the file.

   
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES 128</td>
<td>Place the encryption key, exactly 16 bytes, into the file.</td>
</tr>
<tr>
<td>AES 256</td>
<td>Place the encryption key, exactly 32 bytes, into the file.</td>
</tr>
</tbody>
</table>

3. Update the `edgeencryption.properties` file.
   a) Change to the `<installation directory>/conf/` directory.
   b) Open the `edgeencryption.properties` file.
   c) Enter the properties for the file store.
   d) Save and close the file.

Configure encryption keys on the instance

Edge Encryption provides the tools to manage encryption keys without taking the proxy offline.

Role required: security_admin

Before setting up new encryption keys on the instance:

1. Create the encryption key.
2. Make the new key available to all encryption proxies. Either copy the file or Java KeyStore file to each proxy, or ensure that each proxy has access to the Java KeyStore or Enterprise Key Management (EKM) device.

Key aliases must be unique. Each key alias must have the same key size and type on each proxy, or the key cannot be assigned as the default.

1. Navigate to **Edge Encryption Configuration > Encryption Key Configuration > Set Up Keys**.
2. On the Add New Keys section of the form, complete the following steps to add a new key.

   a) Double-click in the row that says **Insert a new row...**.
   b) In the edit box, enter a name for the key, then click the check mark.
   c) In the same row, double-click in the **Key size** column.
   d) In the select box, select a key size, either **128 bits** or **256 bits**, then click the check mark.
   e) In the same row, double-click in the **Type** column.
   f) In the select box, select a key type, either **File**, **Keystore**, **SafeNet**, or **Unbound**, then click the check mark.
   g) When you are done adding keys, click **Next Step**.
   h) You must specify an alias, key size, and key type for each key before moving on.

3. On the Keys Status section of the form, check the **State** of the key and ensure that it is **Available**. This may take a few minutes. When the key is **Available**, click **Next Step**.

   a) Double-click in the row that says **Retrieve latest key versions** link in the Related Links to retrieve the latest version of each key from the Edge proxy.

   b) In the edit box, enter a name for the key, then click the check mark.
   c) In the same row, double-click in the **Key size** column.
   d) In the select box, select a key size, either **128 bits** or **256 bits**, then click the check mark.
   e) In the same row, double-click in the **Type** column.
   f) In the select box, select a key type, either **File**, **Keystore**, **SafeNet**, or **Unbound**, then click the check mark.
   g) When you are done adding keys, click **Next Step**.
   h) You must specify an alias, key size, and key type for each key before moving on.

The instance tracks the status of every encryption key available to any proxy. When a key is available on all proxies, its state becomes **Available**. If the state does not change after a few minutes, check to ensure that the
key is available on all proxies. If the state remains **Unavailable**, one or more of the proxies does not have the key.

### Encryption key states

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available</td>
<td>All online proxies have the key.</td>
</tr>
<tr>
<td>Unavailable</td>
<td>This is a new key and the proxies have not yet loaded the key, or at least one proxy failed to load the key.</td>
</tr>
</tbody>
</table>

4. On the Change Default Keys section of the form, do one of the following:
   - Type in the key alias.
   - Click the magnifying glass icon and select an alias.

   **Note:** If using SafeNet versioned keys, an additional field appears for the **Key version**. The **Key version** is grayed out and cannot be edited.

   **Note:** If using SafeNet versioned keys, choose only the most recent key version. If you choose an earlier version, the following message appears when you click **Update** or **Next Step**:

   One of the default keys chosen is not the latest version available for the key. Please use the latest version.

   **Note:** If using SafeNet versioned keys, and if the default keys are not the latest versions of the SafeNet keys, an **Update default keys to latest version** link appears in the Related Links. Click the link to update the default keys to use the latest version.

   Click **Next Step**.

5. On the Schedule Key Rotation section of the form, schedule a mass key rotation job or single key rotation job to encrypt existing data using the new encryption key.

   If you do not run a mass key rotation job or single key rotation job, existing data remains encrypted with the old key until the data is accessed again.

Configure additional properties in the Edge Encryption properties file

After installing the Edge Encryption proxy server in your network and setting up your keystore and keys, configure the additional Edge Encryption properties.

1. Open the `<installation directory>/conf/edgeencryption.properties` file and configure the following Edge Encryption proxy server properties:
   - Target (instance) properties
   - User account properties
   - Proxy properties
   - If using order preserving encryption types or encryption patterns, configure the **Proxy database properties**
   - Clear text and static IV properties

2. Save and close the file.
If your network uses a web proxy, you can set up the Edge Encryption proxy to use the web proxy.

If your network does not use a web proxy, leave the web proxy properties in the configuration file commented out.

The Edge Encryption proxy server supports HTTP connection to and basic authentication with the web proxy.

1. Change to the `<installation directory>/conf/` directory.
2. Open the `edgeencryption.properties` file.
3. Configure the web proxy properties.
4. Save and close the `edgeencryption.properties` file.
5. If the web proxy is using a customer-specific server certificate, add this certificate to the JVM used by the Edge Encryption proxy server to establish trust between the web proxy and the Edge Encryption proxy server.
   a) cd to `<Java home directory>/jre/lib/security/cacerts`
   b) Execute the command:
      
      ```
      keytool -keystore cacerts -importcert -alias <chooseAlias> -file <certificateFile>
      ```

Set the proxy server initial memory limit and upper bound memory limit

Set the initial memory limit and upper bound memory limit to specify how much memory the proxy server can consume. Set these limits to avoid performance issues in your Edge Encryption implementation.

As a guideline, set both the initial memory limit and the upper bound memory limit to the same value. On any machine, allocate 2 GB of the physical memory to the operating system (OS). Then allocate the rest of the physical memory to the heap using the initial memory limit and upper bound memory limit properties. For example, on a machine with 8 GB of memory, allocate 2 GB to the OS, and allocate the remaining 6 GB (6144 m) to the initial and upper bound memory.

**Important:** If your Edge Encryption proxy server is running, you must stop and restart the proxy server after updating these properties.

1. In your proxy server directory, open `<install dir>/conf/wrapper.conf`.
2. To set the initial memory limit, add the following line at the end of the file:

   ```
   wrapper.java.additional.<number>=-Xms<min_memory_in_MB>m
   ```

   Set `<number>` to the next available `<number>` in the sequence of `wrapper.java.additional.<number>` properties defined in the `wrapper.conf` file.

   For example, you have the following list of `wrapper.java.additional.<number>` properties:

   ```
   wrapper.java.additional.1=
   wrapper.java.additional.2=
   ```

   The maximum `<number>` in the above list is 2. When you add the `wrapper.java.additional.<number>=-Xms<min_memory_in_MB>m` line, set `<number>` to 3, the next available number.

   **Important:** Do not leave gaps in the numbering sequence.

   Set `<min_memory_in_MB>` to the number of megabytes of memory remaining after allocating 2 GB of memory to the OS.
3. Set the upper bound memory limit.

Because an upper bound memory limit is not set in the base system, the proxy server can use all available memory. If other services are running on the server, you may want to set the upper bound memory limit.

Add the following line at the end of the file:

```java
wrapper.java.additional.<number>=-Xmx<max_memory_in_MB>m
```

Set `<number>` to the next available `<number>` in the sequence of `wrapper.java.additional.<number>` properties defined in the `wrapper.conf` file.

For example, you have the following list of `wrapper.java.additional.<number>` properties:

```java
wrapper.java.additional.1=
wrapper.java.additional.2=
```

The maximum `<number>` in the above list is 2. When you add the `wrapper.java.additional.<number>=-Xmx<max_memory_in_MB>m` line, set `<number>` to 3, the next available number.

**Note:** Do not leave gaps in the numbering sequence.

Set `<max_memory_in_MB>` to the number of megabytes of memory remaining after allocating 2 GB of memory to the OS.

4. Save and close the file.

**Example: Setting proxy server initial and upper bound memory limits**

```java
wrapper.java.additional.1 = -Djava.io.tmpdir=./tmp
wrapper.java.additional.2 = -Dcloudedge.home.dist=..
# must ensure UTF8 encoding when running on Windows
wrapper.java.additional.3 = -Dfile.encoding=UTF8
# additional properties for heap settings
wrapper.java.additional.4 = -Xms6144m
wrapper.java.additional.5 = -Xmx6144m
```

Start the Edge Encryption proxy.

Start the Edge Encryption proxy

After an Edge Encryption proxy is installed and configured, you can start the proxy from the command line.

Before starting the encryption proxy, verify the following:

- The Edge Encryption plugin is activated on the instance.
- The `edgeencryption.properties` file on this machine has been configured.
- If using an order preserving encryption type or encryption patterns, the proxy database is running.
1. Run the proxy server.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>On a Linux machine</td>
<td>a. cd to ServerName_port</td>
</tr>
<tr>
<td></td>
<td>b. Execute ./startup.sh</td>
</tr>
<tr>
<td>On a Windows machine</td>
<td>Perform the following steps from the command line as admin:</td>
</tr>
<tr>
<td></td>
<td>a. cd to ServerName_port/bin</td>
</tr>
<tr>
<td></td>
<td>b. Execute edgeencryption.bat start</td>
</tr>
</tbody>
</table>

2. Check the log on the proxy server to verify that the proxy is running.

Obfuscate passwords in the properties file
You can obfuscate passwords in the edgeencryption.properties file to share the properties file without revealing clear text passwords.

Make sure that the Edge Encryption proxy server is set up and successfully running before you set this property.
Before setting this property, Stop the Edge Encryption proxy.

Setting this property may make it difficult to debug connection and access issues during initial startup. Only set this property in production environments after the proxy has been set up and tested successfully.

1. Change to the <installation directory>/conf/ directory.
2. In the conf directory, create a text file containing a complex string or phrase that can be used as a passphrase which the proxy uses to obfuscate the passwords in the edgeencryption.properties file. This passphrase should be a random and complex phrase not related to the passwords themselves.
3. Open the edgeencryption.properties file.
4. Set the password encryption property.
5. Save and close the edgeencryption.properties file.

After setting this property, you can Start the Edge Encryption proxy.
Manually add an additional proxy
After the first Edge Encryption proxy is properly configured and tested, you can set up additional proxies on a Linux or Windows machine. Installing multiple proxies on the same machine is not recommended.

Add additional proxy servers on additional machines to ensure an optimal environment. See Sizing your Edge Encryption environment to determine the number of additional proxies needed.

Note: Make sure that all proxies have the same encryption keys and the same RSA key pair used to digitally sign encryption configuration and encryption rules. If a proxy database was set up as part of the installation, all proxies must use the same proxy database.

1. Install the proxy using the appropriate command. See Install the Edge Encryption proxy server (interactive installer).
2. Copy all the encryption keys and the edgeencryption.properties file from the first proxy to the new proxy.

Encryption keys may be located in the proxy keystore, in the /keys directory, or in a SafeNet KeySecure keystore.
3. Open the `edgeencryption.properties` file on the new proxy.
4. Change the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>edgeencryption.proxy.name</code></td>
<td>Unique name of the proxy server</td>
</tr>
<tr>
<td><code>edgeencryption.proxy.host</code></td>
<td>The server name, IP address, or fully-qualified domain name of the computer running the proxy.</td>
</tr>
<tr>
<td><code>edgeencryption.proxy.http.port</code></td>
<td>Port on the proxy for HTTP communication. Must be unique across all processes on the machine.</td>
</tr>
<tr>
<td><code>edgeencryption.proxy.https.port</code></td>
<td>Port on the proxy for HTTPS communication. Must be unique across processes on the machine.</td>
</tr>
</tbody>
</table>

5. If installing the proxy server on a Windows machine, you must change the name of the service. Open the `conf/wrapper.conf` file on the new proxy and add the following properties.

   **Note:** You must perform this step before launching the proxy server.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>wrapper.ntservice.name</code></td>
<td>Unique name of the Edge Encryption proxy service.</td>
</tr>
<tr>
<td><code>wrapper.ntservice.displayname</code></td>
<td>Edge Encryption proxy service display name.</td>
</tr>
<tr>
<td><code>wrapper.ntservice.description</code> (Optional)</td>
<td>Proxy server description.</td>
</tr>
</tbody>
</table>

6. Save and close the file.
7. Launch the proxy using the appropriate command. See [Start the Edge Encryption proxy](#)

**Authenticate an Edge Encryption proxy server**

Specify that a proxy server is a trusted source so that Edge Encryption can process requests coming from that proxy server.

If a proxy server is not authenticated, the console log includes the following message:

```
WARN This Edge Encryption proxy has not yet been authenticated by the instance.
Please navigate to the matching Proxy record on your ServiceNow instance and authenticate it.
```

If you attempt to access the proxy, you receive the following message: **This site can't be reached.**

To maintain the proxy in an operational state during the upgrade process, authentication is not required until after the proxy update is successful.

Role required: admin

1. Navigate to **Edge Encryption Configuration > Proxies.**
2. Select the proxy and click **Authenticate.**

The proxy moves from **Unauthenticated** to **Pending** to **Authenticated.** The status changes from **Unauthenticated** to **Pending** when you start the authentication. When authentication is complete, the status changes from **Pending** to **Authenticated,** and you can access the proxy and Edge Encryption can accept requests from the proxy.

   **Note:** If you stop and restart the proxy, the proxy remains **Authenticated** and restarts successfully.
Stop the Edge Encryption proxy
You can stop an Edge Encryption proxy from the command line.

1. Stop the proxy server.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>On a Linux machine</td>
<td>Execute <code>./shutdown.sh</code></td>
</tr>
<tr>
<td>On a Windows machine</td>
<td>Execute <code>edgeencryption.bat stop</code> To remove the Windows service, execute <code>edgeencryption.bat remove</code></td>
</tr>
</tbody>
</table>

2. Check the log on the proxy server to verify that the proxy has stopped.

Uninstall the Edge Encryption proxy on Linux
You can uninstall the Edge Encryption proxy. If you are upgrading the proxy, it is not necessary to shut down and uninstall the current version.

You must have access to the computer running the Edge Encryption proxy.

Before shutting down the Edge Encryption proxy, ensure that no users are connected to the instance using the proxy.

The encryption proxy running on Linux operates as a single process. You can end this process to accommodate such tasks as redeploying the encryption proxy to another host machine, updating the proxy version, updating the Java version, or changing the unique name of the encryption proxy when deploying the encryption proxy on multiple proxy servers.

1. You may want to save the `edgeencryption.properties` file before deleting the distribution directory.
2. Execute the `shutdown.sh` shell script.
3. Check the log on the proxy server to verify that the proxy server is shut down.
4. Delete the files in the distribution folder.

Uninstall the Edge Encryption proxy on Windows
You can uninstall the Edge Encryption proxy. If you are upgrading the proxy, it is not necessary to shut down and uninstall the current version.

You must have access to the computer running the Edge Encryption proxy.

Before shutting down the Edge Encryption proxy, ensure that no users are connected to the instance using the proxy.

1. You may want to save the `edgeencryption.properties` file before deleting the distribution directory.
2. Execute `edgeencryption.bat stop`
3. Execute `edgeencryption.bat remove`
4. Check the log on the proxy server to verify that the proxy server is shutdown.
5. Delete the files in the distribution folder.

Set up multiple provider SSO with Edge Encryption
If implementing multiple provider single sign-on (SSO) with Edge Encryption enabled, some users may need to log in to your instance through the Edge Encryption proxy server, while other users may not. Set up multiple provider SSO to enable logging in through the Edge Encryption proxy server URL or the instance URL.

- Role required: admin
- Enable the Edge Encryption plugin (com.glide.edgeencryption) and ensure that one or more proxy servers are set up in your network.
- Determine the URL for the Edge Encryption proxy server that users will log in through using multiple provider SSO. To determine the URL of an Edge Encryption proxy server, see Edge Encryption installation.
• If routing all users through the Edge Encryption proxy server, set up your identity provider record and define the proxy server URL in the ServiceNow Homepage, Entity ID / Issuer, and Audience URI fields.
• To route some users through the proxy server and some users to the instance, create two identity provider records. Both records use the same value in the Identity Provider URL field. However, one of the records routes through the proxy server, while the other routes to the instance.

1. Enable the duplication of identity provider URLs in identity provider records.
   A unique constraint prevents duplication of the identity provider URL in two different identity provider records. You can enable duplication of the identity provider URL in multiple IdP records by setting a field to false.
   a) Navigate to System Definition > Dictionary.
   b) Open the definition record for the idp field of in the Identity Providers table [saml2_update1_properties].
   c) Configure the form to add the Unique field.
   d) Ensure that the value of the Unique field is set to false.

2. Navigate to Multi-Provider SSO > Identity Providers.
3. Create two identity provider records for the same identity provider: one using the instance URL and one using the Edge Encryption proxy server URL.
   To create an identity provider record, see Create and update identity providers.
   a) For the Edge Encryption proxy server URL, complete the form using these values.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Provider URL</td>
<td>Imported from IdP metadata.</td>
</tr>
<tr>
<td>ServiceNow Homepage</td>
<td>The URL for your proxy server homepage. For example: https://&lt;proxy hostname&gt;:&lt;port&gt;/navpage.do</td>
</tr>
<tr>
<td>Entity ID / Issuer</td>
<td>https://&lt;proxy hostname&gt;:&lt;port&gt;</td>
</tr>
<tr>
<td>Audience URI</td>
<td>https://&lt;proxy hostname&gt;:&lt;port&gt;</td>
</tr>
</tbody>
</table>

b) Click Submit.

c) For the instance URL, complete the form using these values.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Provider URL</td>
<td>Imported from IdP metadata.</td>
</tr>
<tr>
<td>ServiceNow Homepage</td>
<td>https://&lt;instance&gt;.service-now.com/navpage.do</td>
</tr>
<tr>
<td>Entity ID / Issuer</td>
<td>https://&lt;instance&gt;.service-now.com/navpage.do</td>
</tr>
<tr>
<td>Audience URI</td>
<td>https://&lt;instance&gt;.service-now.com/navpage.do</td>
</tr>
</tbody>
</table>

d) Click Submit.
4. Optional: If using more than one identity provider, modify the MultiSSO installation exit.
   a) Navigate to **System Definition > Installation Exits**.
      The system displays the current list of installation exits.
   b) Open the **MultiSSO** installation exit.
   c) Locate the following statement in the **Script** field.

   ```javascript
   var samlResponseTxt = request.getParameter("SAMLResponse");
   if (!GlideSession.get().isLoggedIn() &&
       GlideStringUtil.notNil(samlResponseTxt)) {
       var idpRecord = this.getIdPRecord(request);
       if (idpRecord) {
         SSO_Helper.debug("IdP found based on SAML response: " +
                         idpRecord.getUniqueValue());
         return new SSO_Helper(idpRecord.getUniqueValue(), false, null, true);
       }
   }
   
   d) Replace the statement with the following code.

   ```javascript
   var samlResponseTxt = request.getParameter("SAMLResponse");
   if (!GlideSession.get().isLoggedIn() &&
       GlideStringUtil.notNil(samlResponseTxt)) {
       /* // You have two profiles that use the same IdP entity id it
          cannot use
       // the IdP issuer / entity id from the response otherwise it may
          result in the
       // wrong IdP profile. IdP initiated login will not work
       var idpRecord = this.getIdPRecord(request);
       if (idpRecord) {
         SSO_Helper.debug("IdP found based on SAML response: " +
                         idpRecord.getUniqueValue());
         return new SSO_Helper(idpRecord.getUniqueValue(), false, null, true);
       }*/
       return new SSO_Helper(null, true);
   }
   
   {Note: IdP initiated login does not work in this configuration.}
   
   e) Click **Update**.
5. Optional: If using more than one company, Configure users for Multi-Provider SSO. Update the sys_id of the identity provider record depending on the user.

- To configure a user to log in through the Edge Encryption proxy server, use the sys_id of the identity provider record that uses the Edge Encryption proxy server URL.
- To configure a user to log in to the instance, use the sys_id of the identity provider record that uses the instance URL.

### Login URLs

<table>
<thead>
<tr>
<th>URL</th>
<th>Login destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>https://&lt;instance name&gt;.service-now.com/login_with_sso.do?glide_sso_id=&lt;sys_id of IdP record for the instance URL&gt;</td>
<td>Logs in through the instance.</td>
</tr>
</tbody>
</table>

### Edge Encryption proxy server properties

The `edgeencryption.properties` configuration file located in the `<installation directory>/conf/` folder contains properties used to configure your environment.

You must restart the proxy server after making changes to any proxy server properties. Changes on the instance and changes to the `log4j.properties` do not require a proxy restart.

### Target (instance) properties

**edgeencryption.target.host**

Host name for the instance. Must be the same for all encryption proxies connecting to the same instance. This property is set when the proxy is installed. For example, `instancename.service-now.com`

**edgeencryption.target.port**

Instance port. Must be the same for all encryption proxies connecting to the same instance. This property is set when the proxy is installed.

**edgeencryption.target.protocol**

Instance protocol. Must be the same for all encryption proxies connecting to the same instance. This property is set when the proxy is installed. Options include:

- http
- https

### User account properties

**edgeencryption.target.username**

User name that the proxy uses to log in to the instance. The user must have the edge_encryption role. See Set up an Edge Encryption user account.
edgeencryption.target.password
Password that the proxy uses to log in to the instance.

Proxy properties

edgeencryption.proxy.host
Server name, IP address, or fully qualified domain name of the computer running the proxy. Along with the port, this property defines the URL used by the client to access the proxy server.

dgeencryption.proxy.name
Proxy name. Must be unique for each proxy.

dgeencryption.proxy.http.port
Port on the proxy for HTTP communication.

dgeencryption.proxy.https.port
Port on the proxy for HTTPS communication.

SSL certificate properties

Restart your proxy if you change the value of any SSL certificate property. The system uses the HTTPS keypair on startup to establish the proxy server connection and determine how the proxy answers client requests.

edgeencryption.proxy.https.cert.alias
Alias of the certificate provided by the proxy server to connecting clients.

edgeencryption.proxy.https.keystore.path
Path to the keystore that contains the HTTPS certificate.

edgeencryption.proxy.https.keystore.password
Password for the keystore that contains the HTTPS certificate.

Proxy configuration locked property

edgeencryption.proxy.locked
When true, the proxy does not accept encryption configuration changes or encryption rule changes from the instance. Set this property on the production instance after all encryption configurations and rules are final.

Proxy database properties

edgeencryption.db.url
Proxy database location. Must be the same for all encryption proxies connecting to the same instance.

dgeencryption.db.user
User name for accessing the proxy database. Must be the same for all encryption proxies connecting to the same instance.

dgeencryption.db.password
Password to access the proxy database. Must be the same for all encryption proxies connecting to the same instance.

**edgeencryption.db.name**
Proxy database name. Must be the same for all encryption proxies connecting to the same instance.
- Default value: edgeencryption

**edgeencryption.db.bootstrap.file**
Bootstrap file for the proxy database. The file is relative to the sql/ directory. Must be the same for all encryption proxies connecting to the same instance.

⚠️ **Warning:** Under normal circumstances, do not change this parameter.

**Digital signature properties**

**edgeencryption.proxy.signature.keystore.path**
Path and Java KeyStore file name.

**edgeencryption.proxy.signature.keystore.password**
Password. The default password is <changeme>. Change the password after installing the Java KeyStore.

**edgeencryption.proxy.signature.keystore.keyalias**
The key alias given as the -alias argument when the RSA key pair is generated.

**NAE device keystore properties**

**edgeencryption.nae.retries**
Number of retries to make.

**edgeencryption.nae.enabled**
Setting indicates whether an NAE device is available.

**edgeencryption.nae.server**
Name of the NAE server.

**edgeencryption.nae.port**
Port used by the NAE server.

**edgeencryption.nae.protocol**
Protocol used by the NAE server.

**edgeencryption.nae.keystore.path**
Path to the keystore on the NAE server.

**edgeencryption.nae.keystore.password**
NAE keystore password.

**edgeencryption.nae.username**
User name to use to authenticate with the NAE device.

**edgeencryption.nae.password**
Password to use to authenticate with the NAE device.
**edgeencryption.nae.client.certificate**
Certificate located in the keystore on the NAE server. Set this property to authenticate using a certificate instead of a username and password.

**Clear text and static IV properties**

**edgeencryption.customer.assigned.known.cleartext**
Clear text to let the instance verify that all proxies are using the same keys. At startup, the proxy encrypts the clear text and sends the encrypted text to the instance. The instance does not know the clear text, nor are keys sent to the instance. This property must be the same for all proxies.

**edgeencryption.encrytter.static.iv**
Static IV (initialization vector) used in equality-preserving and order-preserving encryption. This property must be the same for all proxies and must be exactly 16 bytes (16 ASCII characters).

**Password property**

**edgeencryption.encrytter.properties.password**
Name of the file in the conf folder that contains a string used within a secure process to obfuscate passwords in the edgeencryption.properties file.

If this property is not set, passwords in your properties file appear in clear text. Leave this property blank until after the proxy configuration has been set up and tested.

**Web proxy properties**

**edgeencryption.webproxy.host**
Web proxy name or IP address.

**edgeencryption.webproxy.port**
Port on the web proxy.

**edgeencryption.webproxy.user**
User name used to connect to the web proxy. If your web proxy does not use authentication, leave this property commented out.

**edgeencryption.webproxy.password**
Password to use to connect to the web proxy. If your web proxy does not use authentication, leave this property commented out.

**Java KeyStore properties**

**edgeencryption.keystore.path**
Path to the Java KeyStore. If using a file store or a SafeNet KeySecure keystore, leave this property commented out.
Example:

```yaml
edgeencryption.keystore.path = keystore/keystore.jceks
```

**edgeencryption.keystore.password**

Password the proxy uses to connect to the Java KeyStore. If using a file store or a SafeNet KeySecure keystore, leave this property commented out.

### File store property

**edgeencryption.keyfile.directory**

The directory specifies where key files are stored. If using the Java KeyStore or a SafeNet KeySecure keystore, leave this property commented out.

Example:

```yaml
edgeencryption.keyfile.directory=keys
```

If using Unbound Technology keys, uncomment this property and set the value to the keys directory.

### Unbound Technology provider properties

**edgeencryption.ekm.provider.classname**

Internal class name for the implementation.

⚠️ **Warning:** Do not change this property.

**edgeencryption.thirdparty.vendor.library.path**

Path to the Unbound API JAR file on the Unbound client machine.

**edgeencryption.ekm.provider.rsa.wrapping.key.alias**

Wrapping key alias in the Unbound Technology implementation. Must be the same for all proxies.

### General configuration properties

**edgeencryption.config.poll.interval**

Poll interval in seconds. The default setting means that it takes 5 seconds for the proxy to learn of encryption configuration changes. Larger values cause the instance to take longer to detect an offline proxy.

⚠️ **Warning:** Do not change this property. Changing the default setting of the Proxy Poll Interval can result in detection delays when a proxy comes online.

**edgeencryption.rules.dir**

Folder where the encryption rules are stored on the proxy.

**edgeencryption.encryption.order_preserving.cache.enable**

Setting determines whether caching is used to support order-preserving encryption types.
edgeencryption.encryption.order_preserving.cache.size
Maximum cache size, in bytes.

edgeencryption.jobs.concurrency
Maximum number of mass encryption jobs that can run concurrently on this proxy.

edgeencryption.jobs.requests_per_second
Number of http job requests per second that can be sent to the instance by this proxy.

edgeencryption.attachments.request.timeout.seconds
Attachment upload request timeout in seconds.

edgeencryption.request.buffer.size
Size of an encryption request. If an encryption request is larger than this size, the excess is saved to disk.

Warning: Do not change this property.

edgeencryption.httpclient.request.buffer.size
Size of the client request. If the client request is larger than this size, the excess is saved to disk.

Warning: Do not change this property.

edgeencryption.proxy.idle.timeout
Time in seconds after which a transaction times out.
• Default value: 300 (seconds)

edgeencryption.proxy.keepalive.interval
Time in seconds between pings issued by the proxy to the instance. Pings are issued periodically to verify connectivity between the proxy and the instance.
• Default value: 10 (seconds)
• Minimum value: 5 (seconds)

edgeencryption.register.retry.count
Maximum number of times the proxy pings the instance to try to register.
• Default value: 0 (no limit)

edgeencryption.tokenization.exclusion.list
Encryption patterns cannot tokenize strings found in these fields.

Proxy server performance properties

Proxy server performance properties are not present in the configuration file by default. To change the default values, you must add the properties and restart the proxy server. For more information, see Edge Encryption diagnostics and performance.

edgeencryption.stat.collection.enabled
Enables the collection of statistics used by the Edge Encryption proxy server performance dashboard.
• Default value: true

Add this property and set the value to false to disable the collection of statistics used by the Edge Encryption proxy server performance dashboard.

**edgeencryption.stat.collection.interval**

Interval length in seconds during which the Edge Encryption proxy server collects statistics. The value cannot be less than 30 seconds.

• Default value: 30 (seconds)

## Deprecated proxy encryption properties

**edgeencryption.encrypter.default.key128**

Specifies the name of the current AES 128 key. An AES 128 key must be available even if it is not used. Must be the same for all proxies.

Perform maintenance of these keys on the instance.

**edgeencryption.encrypter.default.key256**

Specifies the name of the current AES 256 key. Must be the same for all proxies.

Perform maintenance of these keys on the instance.

**edgeencryption.encrypter.key**

Specifies the key name for each key and is used to specify the default keys. This is the key alias integrated with the metadata that is included with each encrypted item and, therefore, is stored on the instance. The key name must use lowercase letters.

**edgeencryption.encrypter.type**

Specifies the type of encryption keystore system.

**edgeencryption.encrypter.file**

 Specifies the path and file name of the text file associated with the key.

**edgeencryption.encrypter.password**

Specifies the password for accessing the keystore.

---

### CyberArk integration with the Edge proxy server

Use CyberArk to store passwords in a centralized and secure digital vault to secure passwords that were previously stored in clear text and secured by file access, or that were previously encrypted via a second file.

CyberArk AIM (Application Identity Management) prevents unauthorized access by eliminating hard-coded and visible passwords. AIM stores passwords in a digital vault on an independent hardened server, where the passwords are represented as digital credentials. The AIM clients (the Edge proxy servers) use CyberArk digital credentials and access the independent server to retrieve the secured passwords. No passwords are stored on the Edge proxy servers or in the instance.

### CyberArk digital vault credentials

You must purchase and configure CyberArk before you can set up CyberArk integration with the Edge proxy server.

To add a credential to CyberArk (which is read by the Edge proxy), set the **Platform Name** of the credential to **Unix via SSH** and make sure you either create a **Custom** credential **Name** or write down the **Auto-generated**
credential **Name**. When you configure the Edge proxy to use this credential, the proxy server matches this credential **Name** to the setting in the proxy.

Each credential entry holds a **Password** that is being secured, as well as a credential **Name** used by an application to access that password.

**Note:** CyberArk credentials are not encryption keys.

**Adding CyberArk during an Edge proxy installation**

The proxy installer includes a new configuration page for a CyberArk integration. This page is optional if you do not want to include CyberArk when installing your proxy with the proxy installer. You can also manually set up and configure CyberArk integration in the configuration file.
The proxy installer also includes a new page for CyberArk protected credentials. This page allows configurations of different properties using a single credential name or multiple credential names. This page is optional if you do not want to include CyberArk when installing your proxy with the proxy installer.
**CyberArk password protection**

Any password field in the Edge proxy installer that has a CyberArk credential configured in the CyberArk vault and specified on the CyberArk Protected Credentials page of the installer is grayed out and contains the message *Protected by CyberArk.*
Using a load balancer with the Edge proxy server

You can use a load balancer to balance the load across the proxy servers in your Edge Encryption proxy setup. If the load balancer and proxy servers are using different ports, specify the host name and HTTPS port of the load balancer to enable users to view responses on their browser.

**Important:** All production environments should include at least two Edge Encryption proxy servers for redundancy.

Edge request processing without a load balancer

If you are not using a load balancer, a request is processed as described below.

1. The user issues a request from a browser.
2. The browser sends the request to the Edge proxy server.
3. The proxy server sends the request to the ServiceNow instance.
4. The ServiceNow instance returns the response to the proxy server.
5. The proxy server adds its own port number in the response header before returning the response to the user's browser.

The request is completed successfully because the user can view the response from the proxy server at the port number specified in the response header.
Edge request processing with a load balancer

However, if you are using a load balancer, the user’s browser communicates directly with the load balancer, not with the proxy server. A request is processed as described below.

**Note:** The following example uses 1025 as the proxy server port number.

1. The user issues a request from a browser.
2. The browser sends the request to a load balancer Virtual IP (VIP), also known as a Virtual Server.
3. The VIP is configured to point to the proxy server (for example, 10.2.200.148:1025), so the load balancer forwards the request to the proxy server.
4. The proxy server sends the request to the ServiceNow instance.
5. The ServiceNow instance returns the response to the proxy server.
6. The proxy server rewrites the location header in the response with values configured in the properties for risk-servicenow.dev.echonet:1025.
   - **Host:** edgencryption.proxy.host
   - **HTTP port:** edgencryption.proxy.http.port
   - **HTTPS port:** edgencryption.proxy.https.port
7. The proxy server forwards the response to the load balancer with the location header pointing to the proxy server port.

The outcome depends on whether the load balancer and proxy servers are using the same port.
- If the load balancer and proxy servers are using the same port, the request succeeds because the user receives the response from the same port identified in the response header.
- If the load balancer and proxy servers are using different ports, the request fails because the user's browser communicates only with the load balancer, but the response is on the proxy server.

Solution

You could resolve the issue by simply using the load balancer and all Edge proxy servers on the same port, but this is not an ideal solution. A better solution is to enable the system to know which port the load balancer uses.

The following properties enable the Edge proxy server to reroute response messages to the load balancer if the proxy server and load balancer are using different ports.

- **edgeencryption.proxy.rewrite.location.host** specifies the host name used to access ServiceNow through the load balancer.
- **edgeencryption.proxy.rewrite.location.https.port** specifies the HTTPS port used to access ServiceNow through the load balancer.

Configure the load balancer

If the load balancer and proxy servers are using different ports, specify the host name and HTTPS port of the load balancer to enable users to view responses on their browser.

Roles required:

- local or domain administrator on a Windows host
• service user with full file system access on a Linux host

1. Login to the proxy server host as admin, domain admin, or a service user.
2. Navigate to the installation directory for the Edge proxy and select `conf/edgeencryption.properties`.
3. Set the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| `edgeencryption.proxy.rewrite.location.host` | If your Edge configuration includes a load balancer to balance the load among proxy servers, rewrites responses to the load balancer so requests can be completed.  
• If there is a load balancer in the proxy setup, specify the host name used to access ServiceNow through the load balancer.  
• **Optional:** If there is no load balancer in the proxy setup, can be set to the host name used by the proxy server. |
| `edgeencryption.proxy.rewrite.location.https.port` | If your Edge configuration includes a load balancer to balance the load among proxy servers, specifies the HTTPS port used to access ServiceNow through the load balancer.  
• If there is a load balancer in the configuration, specify the HTTPS port used to access ServiceNow through the load balancer.  
• **Optional:** If there is no load balancer in the configuration, can be set to the HTTPS port used by the proxy server. |

4. Save the file.

Requests can be completed because users can now view responses on their browser.

**Edge Encryption upgrades**

Both instance upgrades and proxy server upgrades require special consideration in an Edge Encryption environment.

**Instance upgrades**

Instance upgrades in an Edge Encryption environment require caution to ensure that Edge controls work properly after the instance upgrade.

During an instance upgrade, you should not add, edit, or delete the following:

• Edge Encryption configurations
• Edge Encryption rules
• Edge Encryption tokenization patterns
• Edge Encryption scheduled jobs
• Edge Encryption key configurations
• Edge Encryption scheduled upgrades
• Edge Encryption exclude list IP configurations
Any scheduled job running during the instance upgrade will not complete. To complete the interrupted job, rerun the job once the instance is upgraded. When you reschedule the job, the processing that occurred before the instance upgrade is not lost, and the job continues to process only the data that has not yet been processed.

**Proxy server upgrades**

Schedule a proxy upgrade to enable the instance to upgrade the Edge Encryption proxy server, or manually upgrade the proxy server at any time.

⚠️ **Warning:** For an upgrade on Windows, you may encounter file lock issues and the upgrade may fail. For the upgrade to succeed, you should not have any files open under the installation directory. Also, there should be no existing shell in the installation directory. In particular, if you start the proxy from the command line (via `bin\edgeencryption.bat install/start`) while in the installation directory, you should close that shell or move it out of the installation directory afterward. No files under the installation directory should be opened by an editor or by any other application.

**Third party libraries**

Third party libraries, such as Gemalto, are lost during instance and proxy server upgrades if they are kept in the same directory. You can perform the following to prevent the loss of third party libraries during upgrades:

1. Manually add the following property to `edgeencryption.properties`:
   ```
   edgeencryption.ekm.provider.classname = com.snc.edgeencryption.encryption.CloudEdgeNaeKeyProvider
   ```

2. Add the `edgeencryption.thirdparty.vendor.library.path` vendor library location property and set it to `/path/to/jars`.
   
   For example:
   ```
   edgeencryption.thirdparty.vendor.library.path = /app/servicenow/libs
   ```

3. Copy the SafeNet JARs into that path.

After you install the third party libraries outside of the Edge Encryption installation, they are no longer lost during upgrades.

**Scheduled upgrades**

Schedule an upgrade to allow the instance to upgrade the proxy server at the scheduled time. This functionality is available by default after upgrading. A scheduled upgrade includes these events:

1. The proxy server checks with the instance to see if there is a new version available for upgrade. New versions generally become available when the instance is upgraded.

2. The administrator receives a notification upon logging in when a new version of the proxy server is available.

3. The administrator can Schedule an Edge Encryption proxy server upgrade for each proxy server.

ℹ️ **Note:** Only users with the security_admin role can create an upgrade schedule through the proxy server.
4. Once the upgrade is scheduled, the proxy server automatically upgrades at the scheduled time. During the upgrade, the proxy server is offline for only a short time.

**Note:** Because the proxy server restarts during the upgrade, it is offline for a short time. The amount of time is determined by your environment and how long it takes to stop and restart the proxy service.

5. During the scheduled upgrade, a new proxy directory is created and your configuration files are copied to the new directory. New properties are written to your existing properties file. The following files or directories in your old proxy directory are copied to the new proxy directory:
   - /conf directory
   - /keys directory
   - /keystore directory
   - java/jre/lib/security/cacerts file

As a result, your keys, keystores, settings, and certificates are preserved.

**Note:** Only the above files are copied to the new proxy directory. Any other customized files in the proxy server directory are not preserved during a scheduled upgrade. The upgrade log file can be found in the original proxy directory in the following folder: `<original-proxy-directory>/tmp/upgrade-wrapper/bin`.

### Prerequisites for scheduled upgrades

Before scheduling an upgrade for an Edge Encryption proxy, ensure the following:

1. The `JAVA_HOME` environment variable points to a java installation on the machine that is outside the Edge Encryption proxy’s directory structure.

2. The `JAVA_HOME` environment variable points to a java installation that is at version 1.8_u144 or higher.

3. The `-Djava.io.tmpdir` parameter in the wrapper.conf file of the Edge Encryption proxy points to a directory that is OUTSIDE the Edge Encryption proxy’s directory structure, and the proxy has read/write/execute permissions on the directory. Optionally, you could comment out the parameter entirely so that Java uses its default tmp location.

If you are using Safenet keys, add the following properties to the `edgeencryption.properties` file:

- `edgeencryption.ekm.provider.classname = com.snc.edgeencryption.encryption.CloudEdgeNaeKeyProvider`
- `edgeencryption.thirdparty.vendor.library.path = /path/to/jars`

The `/path/to/jars` has to be outside of the Edge install directory and needs to contain the libraries downloaded from Gemalto:

- `ingrian-log4j-api-2.0-rc1.jar`
- `ingrian-log4j-core-2.0-rc1.jar`
- `ingrian-nae-8.2.0.000.jar`
Manual upgrades

Instead of creating an upgrade schedule, you can manually upgrade each proxy server through the command line. See Manually upgrade an Edge Encryption proxy server running on Linux or Manually upgrade an Edge Encryption proxy server running on Windows.

Proxy build status

You can easily identify whether a proxy server is out of date by navigating to Edge Encryption Configuration > Proxies > All. The status of your proxy build is indicated in the Proxy build column by the following colors:

Green
Your proxy server is up-to-date.

Yellow
Your proxy server is out-of-date and an upgrade is needed.

Orange
Upgrade failed. Your proxy server reverts to the old version to ensure that there is no downtime.

Troubleshoot a failed scheduled proxy upgrade

When a scheduled proxy upgrade fails, the proxy server reverts to the version you are upgrading from. All original data, keys, and configuration files are preserved. This process may take several minutes. Contact Customer Service and Support to ensure a successful upgrade.

To determine the reason for the failure, you can check the Failure Reason in the upgrade schedule. In addition, the installation directory for the failed upgrade is maintained so that log files are available for troubleshooting.
Note: Before deleting any extra proxy directories, always confirm which directory is current by reviewing the log files. If the log files have recent activity, the proxy might be connected to your instance.

If a scheduled proxy upgrade fails repeatedly, you can manually upgrade your proxy server. See Manually upgrade an Edge Encryption proxy server running on Linux and Manually upgrade an Edge Encryption proxy server running on Windows.

Java minimum requirements

The host machine installing or running the Edge Encryption proxy server must maintain a supported version of Java:

- Java 8 update 121 (8u121)
- Java 8 update 141 (8u141)
- Java 8 update 151 (8u151) or later

Note: Java 8 update 131 (8u131) is not supported.

- Java 11.0.6 or later

Note: Before installing the Edge Encryption proxy server, check that the $JAVA_HOME variable is pointing to a supported version of Java for each user that will run the proxy server. For example, if installing the proxy server as a local administrator on Windows, check that the $JAVA_HOME variable is pointing to the correct version of Java system-wide. If installing on Linux, check that each user that will run the proxy server has this variable correctly defined. If a supported version of Java is not found, the Edge Encryption proxy server will not run.

If using AES 256-bit encryption with Java 8 update 141 (8u141) or lower, you must install the Java Cryptography Extension (JCE) jurisdiction policy files by copying them into the system Java home directory of each Edge Encryption proxy server host. Add these files to the <Java-home-directory>/jre/lib/security folder before performing a scheduled or manual upgrade. To install the AES 256-bit encryption policy files, see Enable AES 256-bit encryption for Java 8 update 141 (8u141) or lower.

Mixed proxy-version environments

Although an environment running old versions of the proxy server with up-to-date versions of the proxy server is not recommended, it is supported if all proxy servers are within the same version family as your instance. For example, if you have an instance on the Quebec release, your environment supports proxy servers from any Quebec patch or hot fix. However, the following limitations apply.

- If one proxy server supports functionality that another proxy does not support, you will see inconsistent behavior, depending on which proxy server is used.
- If a proxy server is out-of-date, it may not include recent security enhancements.

If a proxy server from a previous release is registered with a newer release of the instance, you will receive regular notifications that the proxy server is out-of-date. To ensure an optimal and secure environment, ServiceNow recommends always upgrading your proxy server to the most recent version of the software supported by your instance.

Schedule an Edge Encryption proxy server upgrade

Create an upgrade schedule to enable the instance to upgrade an out-of-date proxy server.

To schedule an upgrade, you must be logged in to your instance through the proxy server.
If using AES 256-bit encryption with Java 8 update 141 (8u141) or lower, you must install the Java Cryptography Extension (JCE) jurisdiction policy files by copying them into the system Java home directory of each Edge Encryption proxy server host. Add these files to the `<Java-home-directory>/jre/lib/security` folder before performing a scheduled or manual upgrade. To install the AES 256-bit encryption policy files, seeEnable AES 256-bit encryption for Java 8 update 141 (8u141) or lower.

Role required: security_admin

Once the upgrade is scheduled, the proxy server automatically upgrades at the scheduled time. During the upgrade, the proxy server is offline for only a short time.

**Note:** Because the proxy server restarts during the upgrade, it is offline for a short time. The amount of time is determined by your environment and how long it takes to stop and restart the proxy service.

During the scheduled upgrade, a new proxy directory is created and your configuration files are copied to the new directory. New properties are written to your existing properties file. The following files or directories in your old proxy directory are copied to the new proxy directory.

- `/conf` directory
- `/keys` directory
- `/keystore` directory
- `java/jre/lib/security/cacerts` file

As a result, your keys, keystores, settings, and certificates are preserved.

**Note:** Only the above files are copied to the new proxy directory. Any other customized files in the proxy server directory will not be preserved during a scheduled upgrade. The upgrade log file can be found in the original proxy directory in the following folder: `<original-proxy-directory>/tmp/upgrade-wrapper/bin`.

If multiple proxy servers are out-of-date, you must schedule an upgrade for each proxy server individually.

**Note:** Avoid hosting multiple proxy servers on the same machine. However, if your environment includes this configuration, do not schedule upgrades to multiple proxies on the same machine at the same time.

1. Navigate to **Edge Encryption Configuration > Proxies > Upgrade Schedules**.
2. Click **New**.
3. Complete the form.

### Edge Encryption Proxy Upgrade Schedule form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy server</td>
<td>Proxy server being upgraded.</td>
</tr>
<tr>
<td>Target version</td>
<td>Version to which you are upgrading your proxy server. This value is read-only and set to the most up-to-date proxy version available for your instance.</td>
</tr>
<tr>
<td>Scheduled Start Time</td>
<td>Date and time on which to start the upgrade.</td>
</tr>
<tr>
<td>Active</td>
<td>Whether the scheduled upgrade is active. If this field is not selected, the upgrade will not perform on the scheduled date and time.</td>
</tr>
</tbody>
</table>
Field | Description
--- | ---
Status | The status of the upgrade. This value is read-only. Possible statuses include:
• Pending
• Running
• Complete
• Failed

4. Click **Submit**.

After an upgrade is executed, you can review the upgrade details to learn more about it. If your upgrade failed, review the **Failure Reason** to determine next steps.

**Upgrade details**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Version</td>
<td>The version that the server was upgraded from.</td>
</tr>
<tr>
<td>To Version</td>
<td>The version that the server was upgraded to.</td>
</tr>
<tr>
<td>Actual Start Time</td>
<td>Time that the upgrade began.</td>
</tr>
<tr>
<td>End Time</td>
<td>Time that the upgrade ended.</td>
</tr>
<tr>
<td>Failure Reason</td>
<td>Reason that the upgrade failed.</td>
</tr>
</tbody>
</table>

**Manually upgrade an Edge Encryption proxy server running on Linux**

Update a proxy running on Linux.

If using AES 256-bit encryption with Java 8 update 141 (8u141) or lower, you must install the Java Cryptography Extension (JCE) jurisdiction policy files by copying them into the system Java home directory of each Edge Encryption proxy server host. Add these files to the `<Java-home-directory>)/jre/lib/security` folder before performing a scheduled or manual upgrade. To install the AES 256-bit encryption policy files, see **Enable AES 256-bit encryption for Java 8 update 141 (8u141) or lower**.

Role required: **security_admin** or local administrator on the host machine

1. Copy the Edge Encryption update-archive file to the installation directory.
2. Change to the installation directory.
3. Run the following command:

   ```
   java -jar edgeencryption-dist-<version>-linux-x86-64.jar -m dist-upgrade -c <proxy directory>
   ```

   **Option** | **Description**
   --- | ---
   proxy directory | The directory in the installation directory where the proxy was initially installed. This directory is created by the install.

   If you want to see the help screen, execute this command without arguments: `java -jar edgeencryption-dist-<version>-linux-x86-64.jar`

A new proxy directory is created with a current timestamp. A backup of the old proxy directory is maintained as `backup.dist-upgrade_timestamp` in the new proxy installation directory. The old proxy shuts down and the new proxy starts up. Any open connections/transactions on the old proxy server are terminated.
4. Check the proxy log in the new directory and the instance to verify that the new proxy is running.

**Manually upgrade an Edge Encryption proxy server running on Windows**

Update a proxy running on Windows.

If using AES 256-bit encryption with Java 8 update 141 (8u141) or lower, you must install the Java Cryptography Extension (JCE) jurisdiction policy files by copying them into the system Java home directory of each Edge Encryption proxy server host. Add these files to the `<Java-home-directory>/jre/lib/security` folder before performing a scheduled or manual upgrade. To install the AES 256-bit encryption policy files, see Enable AES 256-bit encryption for Java 8 update 141 (8u141) or lower.

Role required: security_admin or local administrator on the host machine

1. Download the Edge Encryption proxy-update archive file to the installation directory.
2. Start the Windows cmd terminal program with administrator privileges.
3. Change to the installation directory.
4. Run the following command:

   ```
   java -jar edgeencryption-dist-<version>-all.jar -m dist-upgrade -c <proxy directory>
   ```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>proxy directory</td>
<td>The directory in the installation directory where the proxy was initially installed. This directory is created by the install.</td>
</tr>
</tbody>
</table>

If you want to see the help screen, execute this command without arguments: `java -jar edgeencryption-dist-<version>-all.jar`

A new proxy directory is created with a current timestamp. A backup of the old proxy directory is maintained as `backup.dist-upgrade_timestamp` in the new proxy installation directory. The old proxy shuts down and the new proxy starts up. Any open connections/transactions on the old proxy server are terminated.

5. Check the proxy log in the new directory and the instance to verify that the proxy has been updated and is running.

**Roll back an Edge Encryption proxy server upgrade**

If a proxy upgrade is unsuccessful, you can go back to the earlier version.

If an upgrade fails when using the scheduled upgrade feature in the Quebec release, the proxy server will automatically roll back to the old version. The old proxy server is stored unmodified in a backup directory.

If you would like to roll back a manual upgrade, you can follow these steps.

1. Shut down the proxy.
2. Delete the new proxy directory.
3. Rename the backup directory to the proxy name.
   - The backup directory is in the proxy installation directory with the name `<proxy name>_backup`
4. Start the proxy.
5. Check the proxy log and the instance to verify that the proxy is online.

**Edge Encryption configuration**

After the Edge Encryption proxy server is installed and running, manage Edge Encryption through the proxy server.

You must complete all the steps in Edge Encryption installation before creating encryption configurations and encryption patterns on the instance.
Note: To access the Edge Encryption configuration, you must log in through the proxy server and elevate to the security_admin role.

**Rotate encryption keys**
Perform encryption key rotation from the instance. Add a new key, change the default key assignment, and then schedule a mass key rotation or a single key rotation.

Before setting an encryption key as the default key, make the key available to each proxy. This ensures that the proxies have the key to encrypt data when the key is assigned as the default key. All proxies must have access to a key before that key can be assigned as the default key.

**Warning:** Before deleting a key from the proxy, set up and run a mass key rotation job to ensure that no data on the instance uses the key. If any information is still encrypted with that key, you cannot decrypt the information after you delete the key.

**Edge filtering and sorting behavior**
Whenever you change default keys, be sure to perform a key rotation (either mass or single key rotation). Otherwise, you may receive unexpected results when sorting and filtering records. For example, consider the following scenario:

1. You create encrypted records using one encryption key.
2. You create a new key and set it as default.
3. You create a new set of encrypted records using the new encryption key.

If you filter by any encrypted field when connected through the Edge proxy, all records may not be filtered out correctly, or records may appear unexpectedly. The filter works only for records encrypted using the current default key. The records encrypted using the previous default key still appear in the list view.

If you sort by any encrypted field when connected through the Edge proxy, you see two groups of records with the same human readable text in the encrypted field.

**Schedule a single key rotation job**
Schedule a job to find data encrypted using a specified key alias and then re-encrypt the data with the current default encryption key. The data is decrypted before it is re-encrypted with the default key.

Role required: security_admin

Before scheduling this job, update the default key in Edge Encryption Configuration > Encryption Key Configuration > Set Default Keys.

1. Navigate to Edge Encryption Configuration > Maintenance > Schedule Single Key Rotation.
2. Fill in the fields on the form as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a descriptive name.</td>
</tr>
<tr>
<td>Job Type</td>
<td>Select <strong>Single Key Rotation</strong>.</td>
</tr>
<tr>
<td>Key</td>
<td>Enter the key to be retired. Verify that this key is no longer the default key in Edge Encryption Configuration &gt; Encryption Key Configuration &gt; Set Default Keys.</td>
</tr>
<tr>
<td>Estimate record count</td>
<td>Total estimated number of records to process. Not available when running a single key rotation.</td>
</tr>
<tr>
<td>Field</td>
<td>Value</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Process Historical Records</td>
<td>Select to process historical records in the Audit table if the field is audited. When encrypting historical records for a field in the Audit table, both new values and old values are encrypted. This field is read only and active. To learn more about audited fields, see Auditing.</td>
</tr>
<tr>
<td>Estimate Maximum Audit Record Count</td>
<td>Estimated maximum number of audited records to process. Not available when running a single key rotation.</td>
</tr>
<tr>
<td>Active</td>
<td>Clear this check box if you want to deactivate this job.</td>
</tr>
<tr>
<td>Run</td>
<td>Select the period between job executions.</td>
</tr>
<tr>
<td>Starting</td>
<td>Enter the date and time to run the job for the first time.</td>
</tr>
</tbody>
</table>

3. Click the menu icon in the form header and select **Save**.

**Estimate Record Count** is not supported when processing audited fields.

Schedule a mass key rotation job

Schedule a job to find data encrypted with any previous key, and then re-encrypt the data with the current default encryption keys. The data is decrypted before it is re-encrypted with the current default key.

Role required: security_admin

1. Navigate to **Edge Encryption Configuration > Maintenance > Schedule Mass Key Rotation**.
2. Fill in the fields on the form as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a descriptive name.</td>
</tr>
<tr>
<td>Job Type</td>
<td>Select <strong>Mass Key Rotation</strong>.</td>
</tr>
<tr>
<td>Estimate record count</td>
<td>Total estimated number of records to process. Not available when running a mass key rotation.</td>
</tr>
<tr>
<td>Process Historical Records</td>
<td>Select to process historical records in the Audit table if the field is audited. When encrypting historical records for a field in the Audit table, both new values and old values are encrypted. This field is read only and active. To learn more about audited fields, see Auditing.</td>
</tr>
<tr>
<td>Estimate Maximum Audit Record Count</td>
<td>Estimated maximum number of audited records to process. Not available when running a mass key rotation.</td>
</tr>
<tr>
<td>Active</td>
<td>Clear this check box to deactivate this job.</td>
</tr>
<tr>
<td>Run</td>
<td>Select the period between job executions.</td>
</tr>
<tr>
<td>Starting</td>
<td>Enter the date and time to run the job for the first time.</td>
</tr>
</tbody>
</table>

3. Click the menu icon in the form header and select **Save**.

**Estimate Record Count** is not supported when processing audited fields.

Schedule an attachment key rotation job
Schedule a job to find attachments encrypted using a specified key alias, and then re-encrypt the attachments with the current default encryption key. The attachment is decrypted before it is re-encrypted with the default key.

Role required: security_admin

1. Navigate to Edge Encryption Configuration > Maintenance > Schedule Attachment Key Rotation.
2. Fill in the fields on the form as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a descriptive name.</td>
</tr>
<tr>
<td>Job Type</td>
<td>Select Attachment Key Rotation.</td>
</tr>
<tr>
<td>Active</td>
<td>Clear the check mark if you want to deactivate this job.</td>
</tr>
<tr>
<td>Table</td>
<td>Select a table.</td>
</tr>
<tr>
<td>Run</td>
<td>Select the period between job executions.</td>
</tr>
<tr>
<td>Starting</td>
<td>Enter the date and time to run the job for the first time.</td>
</tr>
</tbody>
</table>

3. Click the menu icon in the form header and select Save.
4. To see an estimated count of records to be updated, click Estimated Record Count.
5. To run the job immediately, click Execute Now.

Encrypt fields using encryption configurations
Encrypt fields by creating encryption configurations.

To configure Edge Encryption, you must be connected to the instance through the proxy. Test all changes on a non-production instance before making the changes to the production instance.

Define encryption keys
After setting up one or more proxies and configuring a default encryption key, the instance verifies that the keys are available to all proxies. You cannot make an encryption key the default key unless all proxies have the key. Once a default key is defined, you can create encryption configurations.

Assign fields and attachments to be encrypted
Assigning fields and attachments to be encrypted means assigning an encryption type to the field or attachment. Before marking a field as encrypted, evaluate these issues.

- Determine what system features might be impacted.
- Examine all scripts for use of the field.
- Make any desired adjustments to the field size. After a field has been configured for encryption, the field size cannot be changed.

Marking a field to be encrypted expands the field size to store the encrypted data. The process of expanding the field size can take a long time, depending on the number of records in the table.

Create an encryption configuration
Select the fields to be encrypted and identify the encryption type.

Role required: security_admin

2. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>The table that contains the field to be encrypted.</td>
</tr>
<tr>
<td>Type</td>
<td>Whether to encrypt a table column or attachments for the table. Select <strong>Column</strong>.</td>
</tr>
<tr>
<td>Column</td>
<td>The field to be encrypted. Appears only when the <strong>Type</strong> is <strong>Column</strong>.</td>
</tr>
<tr>
<td></td>
<td>Only String, Date, Date/Time, Journal, Journal Input, and URL fields are supported.</td>
</tr>
<tr>
<td></td>
<td>• <strong>String and URL fields:</strong> You can add an encryption configuration to either a parent table or a child table.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Date and Date/Time fields:</strong> You can add an encryption configuration to a parent table only. You cannot add a new encryption configuration to a child table.</td>
</tr>
<tr>
<td>Encryption type</td>
<td>The encryption type to use.</td>
</tr>
</tbody>
</table>

**Note:** Depending on the number of records affected by the Date and Date/Time fields you are encrypting, it may take up to a few minutes to create the encryption configuration. Make sure that you create the encryption configuration for Date and Date/Time fields when transaction volume on the instance is low.

| note: A specific table and field combination can have only one active configuration at a time. |

3. Click **Submit**.

After you add the encryption configuration record, you can create an encryption job to encrypt existing data. If you do not run an encryption job, Edge encrypts the existing data the next time the data changes.

Deactivate an encryption configuration

After configuring a field or a table's attachments to be encrypted, you can stop encryption by deactivating the encryption configuration. After deactivating encryption, you can run a Decryption job for fields or an Attachment Decryption job for attachments to remove the encrypted data from the instance.

Role required: security_admin

**Warning:** Deactivating an encryption configuration does not delete the encryption record and the encryption type cannot be changed.

1. Navigate to **Edge Encryption Configuration > Edge Encryption Configurations > All**.
   The **Edge Encryption Configurations** list is shown.
2. Click on the encryption configuration to be deactivated.
   The **Edge Encryption Configuration** form is shown.
3. Click on the **Active** box.
   The **Active** box is clear.
4. Click **Update**.
   
The *Edge Encryption Configurations* list is shown.

You can run a Decryption or Attachment Decryption job to decrypt data on the instance. If you do not run a job, the encrypted data is decrypted the next time it is changed.

**Schedule an encryption job**

You can schedule a job to find and encrypt any unencrypted data in a specified field, using the default encryption key configured for the field. If you do not create an encryption job after configuring a field for encryption, only new values are encrypted.

Role required: security_admin

1. Navigate to *Edge Encryption Configuration > Encryption Configurations > All*.

2. Click the field that you want to schedule an encryption job for.


   The *Scheduled Encryption Job* form is shown with all fields populated. The bottom of the form shows records for any previous job executions.

4. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a descriptive name.</td>
</tr>
<tr>
<td>Active</td>
<td>Clear this check box if you want to deactivate this job.</td>
</tr>
<tr>
<td>Job Type</td>
<td>Select <strong>Encryption</strong>.</td>
</tr>
<tr>
<td>Table</td>
<td>Select a table.</td>
</tr>
<tr>
<td>Column</td>
<td>Select a column.</td>
</tr>
<tr>
<td>Estimated record count</td>
<td>Total estimated number of records to process. Populates after selecting <strong>Estimate Record Count</strong>.</td>
</tr>
<tr>
<td>Process Historical Records</td>
<td>Select to process historical records in the Audit table if the field is audited. When encrypting historical records for a field in the Audit table, both new values and old values are encrypted. To learn more about audited fields, see <strong>Auditing</strong>.</td>
</tr>
<tr>
<td>Estimate Maximum Audit Record Count</td>
<td>Estimated maximum number of audited records to process. Populates after selecting <strong>Estimate Record Count</strong>. This field is only visible when <strong>Process Historical Records</strong> is selected.</td>
</tr>
<tr>
<td>Run</td>
<td>Select the period between job executions.</td>
</tr>
<tr>
<td>Starting</td>
<td>Enter the date and time to run the job for the first time.</td>
</tr>
</tbody>
</table>

5. Click the menu icon in the form header and select **Save**.

6. To see an estimated count of records to be updated, click **Estimate Record Count**.

7. To run the job immediately, click **Execute Now**.

---

© 2021 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
You can schedule a job to decrypt data in an encrypted field, to store clear data in the instance.

**Note:** You must mark the encryption record for the field as inactive (clear the **Active** box) in order to run the decryption job.

**Important:** Access is required to encrypted data prior to running a mass decryption. If your instance contains encrypted column and/or attachments with encryption contexts, Key Management Framework, or Platform Encryption, first assign the encryption contexts or cryptographic modules to the instance user that is configured in the Edge Encryption config file.

Role required: **security_admin**

1. Navigate to **Edge Encryption Configuration > Encryption Configurations > All.**
2. Click the field that you want to decrypt.
3. Under **Related Links**, click **Schedule Mass Decryption Job.**

   The **Scheduled Encryption Job** form is shown with all fields populated. The bottom of the form shows records for previous job executions.

4. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a descriptive name.</td>
</tr>
<tr>
<td>Job Type</td>
<td>Select <strong>Decryption.</strong></td>
</tr>
<tr>
<td>Active</td>
<td>Clear this check box if you want to deactivate this job.</td>
</tr>
<tr>
<td>Table</td>
<td>Select a table.</td>
</tr>
<tr>
<td>Column</td>
<td>Select a column.</td>
</tr>
<tr>
<td>Estimated record count</td>
<td>Total estimated number of records to process. Populates after selecting <strong>Estimate Record Count.</strong></td>
</tr>
<tr>
<td>Process Historical Records</td>
<td>Select to process historical records in the Audit table if the field is audited. When encrypting historical records for a field in the Audit table, both new values and old values are encrypted. To learn more about audited fields, see Auditing.</td>
</tr>
<tr>
<td>Estimate Maximum Audit Record Count</td>
<td>Estimated maximum number of audited records to process. Populates after selecting <strong>Estimate Record Count.</strong> This field is only visible when <strong>Process Historical Records</strong> is selected.</td>
</tr>
<tr>
<td>Run</td>
<td>Select the period between job executions.</td>
</tr>
<tr>
<td>Starting</td>
<td>Enter the date and time to run the job for the first time.</td>
</tr>
</tbody>
</table>

5. Click the menu icon in the form header and select **Save.**
6. To see an estimated count of records to be updated, click **Estimate Record Count.**
7. To run the job immediately, click **Execute Now.**
Encrypt attachments using standard encryption

You can encrypt attachments for specific tables.

All attachments to a table use the same encryption type. Encrypted attachments are not searched when performing a text search. Only the standard encryption types are allowed for attachments. The order preserving or equality preserving encryption types are not allowed.

For a session bypassing the Edge Encryption proxy:

- On a record with attachment encryption activated:
  - The user can see that there are attachments and the attachment names.
  - The user cannot add new attachments.
- On a record without attachment encryption activated:
  - The user can open and download existing attachments.
  - The user can add new attachments.

For a session using the encryption proxy, the user can open and download existing attachments and add new attachments.

Configure attachment encryption

Select the tables whose attachments are to be encrypted and identify the encryption type.

Role required: security_admin

2. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>Select a table whose attachments are to be encrypted.</td>
</tr>
<tr>
<td>Type</td>
<td>Whether to encrypt a table column or attachments for the table. Select Attachment.</td>
</tr>
<tr>
<td>Column</td>
<td>The table field to be encrypted. This field appears when the Type is Column, and not when Type is Attachment.</td>
</tr>
<tr>
<td>Encryption type</td>
<td>The encryption type to use. For attachments, only Standard AES128 and Standard AES256 are allowed.</td>
</tr>
</tbody>
</table>

3. Click Submit.

After the encryption record has been added, you can create an attachment encryption job to encrypt existing attachments. If you do not run an attachment encryption job, the system encrypts new attachments when you attach them.

Schedule an attachment encryption job

You can schedule a job to find and encrypt any unencrypted attachments for a specified table, using the default encryption key configured for the table.

Role required: security_admin

1. Navigate to Edge Encryption Configuration > Encryption Configurations > All.
2. Click the table you want to schedule an encryption job for.

The Scheduled Encryption Job form is shown with all fields populated. The bottom of the form shows records for previous job executions.

4. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a descriptive name.</td>
</tr>
<tr>
<td>Active</td>
<td>Clear this check box if you want to deactivate this job.</td>
</tr>
<tr>
<td>Job Type</td>
<td>Select Attachment Encryption.</td>
</tr>
<tr>
<td>Table</td>
<td>Select a table.</td>
</tr>
<tr>
<td>Run</td>
<td>Select the period between job executions.</td>
</tr>
<tr>
<td>Starting</td>
<td>Enter the date and time to run the job for the first time.</td>
</tr>
</tbody>
</table>

5. Click the menu icon in the form header and select Save.
6. To see an estimated count of records to be updated, click Estimate Record Count.
7. To run the job immediately, click Execute Now.

Schedule an attachment decryption job

You can schedule a job to decrypt any encrypted attachments for a specified table, to store clear attachments in the instance.

Note: You must mark the encryption record for the table as inactive (clear the Active box) before the decryption job runs, otherwise, nothing happens.

Role required: security_admin

1. Navigate to Edge Encryption Configuration > Encryption Configurations > All.
2. Click the table with the attachments that you want to decrypt.

The Scheduled Encryption Job form is shown with all fields populated. The bottom of the form shows records for previous job executions.

4. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a descriptive name.</td>
</tr>
<tr>
<td>Job Type</td>
<td>Select Attachment Decryption.</td>
</tr>
<tr>
<td>Active</td>
<td>Clear the check mark if you want to deactivate this job.</td>
</tr>
<tr>
<td>Table</td>
<td>Select a table.</td>
</tr>
<tr>
<td>Run</td>
<td>Select the period between job executions.</td>
</tr>
<tr>
<td>Starting</td>
<td>Enter the date and time to run the job for the first time.</td>
</tr>
</tbody>
</table>

5. Click the menu icon in the form header and select Save.
6. To see an estimated count of records to be updated, click Estimate Record Count.
7. To run the job immediately, click Execute Now.
Change a field or attachment’s encryption type
You can change a field or attachment’s encryption type by selecting a new encryption type in the existing encryption configuration record. A specific table and field combination can only have one active configuration at a time.

Role required: security_admin

1. Navigate to Edge Encryption Configuration > Encryption Configurations > All. The Edge Encryption Configurations list is shown.
2. Open the record for the encryption configuration to be changed.
3. Click the Encryption type dropdown and select a new encryption type.

   ![Note: For attachments, only Standard AES128 and Standard AES256 are allowed.]

4. If needed, run an encryption or attachment encryption job. It is not necessary to run an encryption job. If you do not run an encryption job, the field or attachment is encrypted using the new encryption type the next time the field or attachment is changed.

Tokenize strings using encryption patterns
You can replace string patterns with tokens before they are sent to and stored in the instance.

To use encryption patterns, you must install and set up a MySQL database in your network. This is the same database used for order-preserving encryption. To create or edit encryption patterns, you must be connected to the instance through the proxy.

Role required: security_admin

You can use base system patterns, or create your own patterns. Base system patterns are advanced patterns. Encryption patterns include the following limitations.

• A pattern of all alpha characters is not allowed.
• The minimum pattern size is five characters. You can change this setting using a system property.
• The * and + quantifiers are forbidden in encryption patterns.
• Encryption patterns match complete words, not parts of strings embedded in a larger string. Words are defined by spaces and characters not available for inclusion in a pattern.
• If the same string is sent to the instance multiple times, it is replaced with the same token.
• Text search on exact matches is supported. The query string is exchanged with a token when sent to the instance, the search is performed on tokens, and when the search results are returned to the proxy server, the tokens are replaced with the clear text. Features such as stemming are not supported.

When using patterns, the clear text never leaves your network. When the proxy server matches a pattern in a request going to the instance, the proxy replaces the string with a token of the same size. The token is sent to instance instead of the clear text string. When the response is sent from the instance to the proxy server, the proxy replaces the token with the string. When viewed through the proxy server, the string displays as clear text.

   ![Note: Encrypted fields are not checked for encryption patterns.]

1. Navigate to Edge Encryption Configuration > Encryption Patterns > Create New. Alternatively, you can navigate to Advanced Patterns to activate or edit a preconfigured pattern.
2. Enter the pattern name.
3. Define the **Edge pattern input type**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basic</strong></td>
<td>A series of character types. In the Basic Pattern Input tab, click Add and select a character type. The Sample pattern displays the pattern as characters are added. Click New Block to move the next character to the next line. This enables you to group characters in a long pattern. Click X to delete the last character in the pattern.</td>
</tr>
<tr>
<td><strong>Advanced</strong></td>
<td>A Java RegEx expression. If advanced is selected, you cannot change the input type back to basic. In the Sample match field, enter a sample pattern to test the RegEx expression. In the Pattern field, enter a Java RegEx expression. Click Validate to verify that the expression matches the sample pattern.</td>
</tr>
</tbody>
</table>

The input type defines how you are going to enter the pattern. It does not impact how the pattern is used.

4. Click **Submit**.

**Repair or recover order-preserving encrypted data**

If you have the security-admin role, you can schedule jobs performed by the Edge Encryption proxy to repair or recover fields that use order preserving encryption.

You can schedule jobs to:

- Repair order tokens.
- Recreate the proxy database.

Running these jobs can be a time-consuming operation which might impact the performance of the Edge Encryption proxy. Schedule these jobs at a time when no users or a minimum set of users are using the system, such as midnight on the weekend.

**Schedule an order token repair job**

You can schedule a job to find and repair fields where the order token is missing.

Role required: security_admin

Use these jobs to repair individual fields in a table or to repair all fields using order preserving encryption. Run this job when the proxy database has been offline while the instance has been running, which results in order preserving fields that are missing order tokens.

1. Navigate to **Edge Encryption Configuration > Maintenance > Schedule Order Token Repair**.
2. Fill in the fields on the form, as appropriate.
Schedule a proxy-database recovery job

Run this job when the proxy database has lost data. This job finds all records that have been encrypted with a token (order preserving encryption type) and sends them to the proxy so that the proxy database can be rebuilt.

Role required: security_admin

1. Navigate to **Edge Encryption Configuration > Maintenance > Schedule Database Recovery**.
2. Fill in the fields on the form, as appropriate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a descriptive name for this job.</td>
</tr>
<tr>
<td>Job Type</td>
<td>Select <strong>Database Recovery</strong>.</td>
</tr>
<tr>
<td>Active</td>
<td>Clear this check box if you want to deactivate this job.</td>
</tr>
<tr>
<td>Run</td>
<td>Select the period between job executions.</td>
</tr>
<tr>
<td>Starting</td>
<td>Enter the date and time to run this job for the first time.</td>
</tr>
</tbody>
</table>

3. Click the menu icon in the form header and select **Save**.
4. To see an estimated count of records to be updated, click **Estimated Record Count**.

Prevent an IP address in your network from sending requests to your instance

Because the Edge Encryption proxy server resides in your network, it may be subject to vulnerability scans by your network software. To prevent IP scanner or other requests from being forwarded to your ServiceNow instance, you can add IP addresses, IP ranges, or network masks to a deny list. Any connection to the proxy server from a deny listed address is terminated and is not forwarded to your instance.

Role required: security_admin

To place an IP address on a deny list, you must be logged in to your instance through the proxy server.

**Important:** Ensure that you understand your network topology before adding IP addresses in your network to a deny list. If an IP address is added to the deny list, any user with that IP address will be blocked from accessing the Edge Encryption proxy server.

1. Navigate to **Edge Encryption Configuration > Maintenance > Denylist IP Addresses**.
2. Click **New**.
3. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy server</td>
<td>The Edge Encryption proxy server that is prevented from forwarding requests from addresses on the deny list.</td>
</tr>
</tbody>
</table>
4. Click **Submit**.
5. Repeat these steps for all other proxies for which an IP address should be denied.

The Edge Encryption proxy server terminates any connection from IP addresses, ranges, or network masks on the deny list and cannot forward the request to the instance. **Encrypt data from a record producer**

Record producers allow end users to create task-based records, such as incident records, from the Service Catalog and Service Portal. If a record producer attempts to insert data into a field marked for encryption, an invalid insert message displays and the data is not saved to the field. To configure your Edge Encryption proxy server to allow inserts from a record producer, create encryption rules from the record producer record.

**Role required: security_admin**

Encrypting data from a record producer requires an encryption configuration defined for the target field. Check that you have created an encryption configuration for the target field and table before creating an encryption rule from a record producer. See **Create an encryption configuration**. To encrypt attachments from a record producer, **Configure attachment encryption**.

1. Log in to your instance through the Edge Encryption proxy server.
2. Navigate to **Service Catalog > Catalog Definitions > Record Producers**.
3. Create a record producer record or open an existing record producer record.
4. Under **Related Links**, select **Create Edge Encryption Rule**.

Two inactive encryption rules are automatically created to encrypt data sent from the record producer to the field marked for encryption.

<table>
<thead>
<tr>
<th>Encryption rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;RecordProducerName&gt;</code></td>
<td>Rule created to process POST parameters from the Service Catalog and map variables to fields in the instance.</td>
</tr>
<tr>
<td><code>&lt;RecordProducerName&gt;Json</code></td>
<td>Rule created to process a JSON payload from the Service Portal and map variables to fields in the instance.</td>
</tr>
</tbody>
</table>

5. Activate the necessary encryption rules created by the record producer.
   a) Navigate to **Edge Encryption Configuration > Rules > All**.
   b) Depending on where the record producer will be used, open the associated encryption rule created by the record producer and select the **Active** flag.

If using the record producer in the Service Catalog, activate the `<RecordProducerName>` encryption rule. If using the record producer in the Service Portal, activate the `<RecordProducerName>Json` encryption rule.
6. Optional: Examine the Encryption rule Action field and add any necessary field names or statements.

If a record producer directly maps a variable to a field in a table, the encryption rule automatically maps the variable to the correct field. However, if a variable is indirectly mapped through various scripts on the platform, you may need to update the rules to map each variable to the correct field.

The below encryption rule was created from the Report Outage record producer and processes POST parameters from the Service Catalog to map variables to fields in the instance. Replace 'FILL ME IN' with the target field.
The below encryption rule was created from the Report Outage record producer and processes a JSON payload from the Service Portal to map variables to fields in the instance. Add additional statements to map any scripted variables to the target fields.
Edge Encryption Rule

ReportOutage.js

<table>
<thead>
<tr>
<th>Name</th>
<th>ReportOutage.js</th>
<th>Request type</th>
<th>HTTP Post</th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Action</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Order</td>
<td></td>
<td></td>
<td>100</td>
</tr>
</tbody>
</table>

```javascript
function ReportOutageJsonCondition(request) {
  return true;
}
```

```javascript
function ReportOutageJsonAction(request) {
  var tableName = 'INCIDENT';
  var isCurrentConfiguration = request.getParameter('variable1');
  if (isCurrentConfiguration) {
    return false;
  }
  return true;
}
```
When the payload from the record producer is examined, the error_message element contains the value for the short_description field. By adding the following statement, you can map the scripted variable error_message to the short_description field.

```javascript
if (jsonElement.getName() == 'error_message')
    jsonElement.valueFor(tableName, 'short_description');
```

The value of the Action field becomes:

```javascript
function ReportOutageJsonAction(request) {
    var tableName = 'incident';
    // Some fields are set in script, additional parameter lines may need to be added
    // current.comments is accessed via script from notes; // assignment to current.comments does NOT replace existing values
    // current.short_description is accessed via script from short_description;
    // current.description is accessed via script from current.short_description;
    // current.caller_id is accessed via script from gs.getUserID();
    var jsonContent = request.getAsJsonContent();
    for (var jsonElementItr = jsonContent.getIterator('variables'); jsonElementItr.hasNext();)
    {
        var jsonElement = jsonElementItr.next();
        if (jsonElement.getName() == 'error_message')
            jsonElement.valueFor(tableName, 'short_description');
        else {
            jsonElement.valueFor(tableName, jsonElement.getName());
        }
    }
}
```

The two encryption rules enable the record producer to insert values into fields marked for encryption from either the Service Catalog or Service Portal.

**Define a custom encryption rule**

It may be necessary to identify and encrypt sensitive information in HTTP requests on the way to your instance. You can write encryption rules to identify, interpret, and encrypt data in such requests, mapping fields in the request to table-field names on your instance.

**What is an encryption rule**

Encryption rules are scripts executed on the Edge Encryption proxy server to map fields in a request to fields in a table on your ServiceNow instance. An encryption rule tells the Edge Encryption proxy server how to encrypt data in custom payloads.

**Note:** Encryption rules only support ECMAScript 3 and below.

**When to use custom rules**

A set of encryption rules is included as part of the Edge Encryption plugin. These rules handle core platform use cases such as editing a field from the list edit form, updating a record from the record form, managing direct web services, and processing data from the REST API. Applications created using standard forms and lists should work without custom encryption rules.

If you develop scripted processors, scripted web services, scripted REST APIs, UIs, or Ajax scripts that contain data that should be encrypted, you must write encryption rules to find and map the data to Glide table-field names.
Format of an encryption rule

Rules include three parts:

- **Condition**: Identifies the type of request.
- **Action**: Maps fields in the request to fields in a table, encrypting values that map to fields with encryption configurations defined.
- **Order**: Priority of the rule. The lowest priority rule with a satisfied condition is the only rule that runs. Like business rules, rules run from lowest to highest.

Except for attachment requests, when an HTTP request hits the Edge Encryption proxy server, the Edge Encryption proxy server evaluates all encryption rule conditions in priority order until either all conditions return false, or one condition returns true. When a condition returns true, the action is executed on the request and the result is forwarded to the instance. No other conditions are evaluated. As a result, encryption rule conditions should be as specific as possible. A generic rule might evaluate as true for a request meant to be processed by another rule, causing the request to be processed by the wrong action. If a generic condition is unavoidable, the rule should be marked with a high-order value so that more specific rules are evaluated first.

Guidelines for creating encryption rules

Creating efficient, optimized encryption rules can reduce processing time for script validation.

**Overall guideline**: When rules get very long, do your best to minimize the number of blocks and break the rules apart whenever possible. Ideally, custom rules should apply to specific use cases, rather than encompassing several cases, with `if`s or switch statements in the action script.

1. Split rules whenever possible. For example,
   - Create different rules for different tables and ensure that each rule runs only on its respective table.
   - Create different rules for each record producer you are targeting, or at least for each subset of record producers. Instead of one rule targeting dozens of `sys_ids`, you could create several different rules targeting smaller subsets of record producers, or even create one rule per `sys_id`.

   **Note**: Creating multiple rules requires more maintenance. The trade-off is that multiple, simpler rules can be validated more efficiently than longer, more complex rules.

2. Minimize the number of blocks. Because the processing engine scans each block while evaluating scripts, a large number of blocks causes delays in validation. For example,
   - Replace all `if` blocks with an array lookup, and replace all blocks in the array lookup with just one `if` block.
   - Combine `if` blocks whenever it is possible to group them.

Encryption rule APIs

Encryption rules are written in JavaScript and utilize Edge Encryption APIs to locate and encrypt sensitive information in the body of a request. The API uses expressions similar to xPath to navigate through both JSON and XML content.

Edge Encryption APIs process the request off the stream as it is being written to the output stream. Stream parsing allows encryption rules to be network performant. However, fetching and parsing content from the body multiple times could lead to unexpected results. To account for this, requests should be processed by the action in a single pass.
When creating encryption rules, you cannot use Glide APIs, script includes, business rules, or any global parameters such as `current`. Because the rules are created for HTTP objects, a global `request` object is available.

When creating encryption rules, you cannot use APIs from the white list manager or scoped applications.

**Error handling**

If an encryption rule condition or action throws an exception, check the proxy log for troubleshooting information.

**Inspect the client request**

Before creating a custom encryption rule, you must determine the format of the client request entering the Edge Encryption proxy server.

Because encryption rules iterate over client requests and determine what, if anything, needs to be encrypted, you must understand the type of request you are creating a rule for. The format of the client request determines the structure of your encryption rule and the APIs available for use in the rule.

1. Inspect the client request.

   Depending on the source of the request, the following tools are available to inspect the request and determine the format.

<table>
<thead>
<tr>
<th>Source of request</th>
<th>Available tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client browser</td>
<td>Use the developer console in your browser to inspect the client request. Useful tools include:</td>
</tr>
<tr>
<td></td>
<td>• Firefox Network Monitor</td>
</tr>
<tr>
<td></td>
<td>• Chrome Network Panel</td>
</tr>
<tr>
<td>Third-party/external source</td>
<td>Use an HTTP protocol analyzer to inspect the request. Useful tools include:</td>
</tr>
<tr>
<td></td>
<td>• Wireshark</td>
</tr>
<tr>
<td></td>
<td>• HTTP Scoop</td>
</tr>
<tr>
<td></td>
<td>Alternatively, you can often use documentation for the external source to determine the format of the request.</td>
</tr>
</tbody>
</table>
2. From the client request, inspect the packet and determine:
   • The client request method
   • The URL path of the request
   • The URL parameters
   • The POST parameters, if any
   • The format of the request body, if included

Inspecting the request provides an understanding of the fields you need to filter for and iterate over in your encryption rule. To understand the fields in the request object, see request.

Create an encryption rule
Encryption rules are used by the proxy to find content in HTTP requests that should be encrypted.

Role required: security_admin

Before creating an encryption rule, you must Inspect the client request to determine the format.

To create or edit encryption rules, you must be connected to the instance through an encryption proxy.

1. Navigate to Edge Encryption Configuration > Rules > Create New.
2. In the Name box, enter a name.
3. In the Request Type, select an HTTP method.
   • HTTP Post
   • HTTP Get
   • HTTP Put
   • HTTP Patch
   • HTTP Delete

   **Note:** Pre-Jakarta instances allow only HTTP Get and HTTP Post methods.

4. In the Condition box, enter a JavaScript statement defining when the rule should run.
5. In the Action box, enter a JavaScript function to be executed when the condition is true.
6. In the Order box, enter the relative priority of the rule.
7. Click Submit, or save the form.

Encryption rule conditions
Encryption rule conditions determine if the rule should be executed.

An encryption rule condition must return true if the rule is to handle the HTTP request; otherwise, it must return false.

As you build your condition, keep in mind that only one rule is executed per request. As a result, the condition must be as general or specific as needed to run under the intended circumstances.
Note: Be careful when performing checks on content in the condition. Excessive checks can be expensive for the proxy server and may cause increased latency when handling complex requests.

The condition can use the method type, content type, URL path, or any URL query string parameters to determine if the rule should handle the request. The condition has access to these fields via the request object. Be sure that, prior to creating an encryption rule condition, you have inspected the client request and understand the conditions needed to trigger the rule.

Note: To build efficient rules, consider easy ways to rule out requests that you do not want to be evaluated by a rule. Build your condition to return false for those requests first. This method increases performance and quickly routes the request to the correct rule faster.

Encryption rule objects and APIs are available to encryption rule conditions.

Example using path and postParams

```javascript
/*This condition checks if the request coming in has a path ending in "/sample_processor.do" and if a post parameter exists in that request called myPostParam */

function SampleCondition(request) {
  if (endsWith(request.path, "/sample_processor.do") && request.postParams.myPostParam) {
    return true;
  }
  return false;
}
```

Example using urlParams and contentType

```javascript
/* This condition checks if a url parameter exists in the query called myUrlParam and if the content type contains 'xml' (if so, you can expect the body to be an XML payload). Then, it checks if the xml payload contains myXmlTag */

function SampleCondition2(request) {
  if (request.urlParams.myUrlParam && request.contentType.indexOf('xml') > -1 && request.xmlContains('myXmlTag')) {
    return true;
  }
  return false;
}
```

Encryption rule actions

An encryption rule maps fields in a client request to fields in a table on your instance and identifies fields marked for encryption.

An encryption rule action only runs when the encryption rule condition returns true. An encryption rule identifies the data to be encrypted in your request payload. Because the rule iterates over the content in the request object, you must understand the form and structure of your request body and determine what in the request needs to be encrypted. The data to be encrypted might be located within:

- A POST or URL parameter.
- JSON or XML content within a POST or URL parameter.
- A JSON payload.
Before writing an encryption rule action, be sure to:

- Inspect the client request.
- Identify where the sensitive data is located in the request object.
- Determine the field and table name to insert data into, or understand how to dynamically pull this from the request.

Encryption rule objects and APIs are available to encryption rule actions and conditions.

Encryption rule objects and APIs
Use encryption rule APIs to parse and encrypt values in requests moving through the Edge Encryption proxy server to the instance.

The APIs available for your encryption rule depend on the format of the request object. For example, if the contentType parameter of the request object is XML, you can use the XML APIs to parse and encrypt values in the payload. After you determine the type of object in your request, you can build an encryption rule using the available APIs.

Encryption rule APIs are available in both encryption rule condition and action scripts.

request
The request object is a global object available in Edge Encryption rule action and condition scripts.

The request object is a JavaScript object that represents the client request coming in to the Edge Encryption proxy server. You must build your encryption rule to parse the request object, map request object values to fields in a table on the instance, and encrypt any sensitive data in the request object.

The request object includes the following attributes and data from the client request:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>path</td>
<td>The path portion of the URL</td>
</tr>
<tr>
<td>requestMethod</td>
<td>GET, POST, PUT, PATCH, DELETE.</td>
</tr>
<tr>
<td>contentType</td>
<td>The Content-Type header field.</td>
</tr>
<tr>
<td>urlParams</td>
<td>The parameters in the query string. This can also be evaluated to a String.</td>
</tr>
<tr>
<td>postParams</td>
<td>If this is a form post, this contains the post parameters.</td>
</tr>
</tbody>
</table>

request - getAsJsonContent()

Returns the request as an iterable object of type JsonNode.

This method is available only in an Edge Encryption rule if the request body is a valid JSON payload. If you are not sure what format the request body includes, check the contentType field on the request object.

Once the request is returned as a JsonNode object, you can use the JSON APIs to iterate over the object and encrypt fields.

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>JsonNode</td>
<td>The request as an iterable JsonNode.</td>
</tr>
</tbody>
</table>

request - `getAsXmlContent()`

Returns the request content as an iterable object of type `XMLContent`.

This method is available only in an Edge Encryption rule if the request body is a valid XML payload. If you are not sure what format the request body includes, check the `contentType` field on the `request` object.

Once the request is returned as an `XMLContent` object, you can use the XML APIs to iterate over the object and encrypt fields.

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>XMLContent</td>
<td>The request as an iterable object of type <code>XMLContent</code>.</td>
</tr>
</tbody>
</table>

request - `XMLContains(String path)`

Returns true if the given path exists in the XML DOM.

This method is available only if the request body is a valid XML payload. If you are not sure what format the request body includes, check the `contentType` field on the `request` object.

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>path</td>
<td>String</td>
<td>XPath statement you are searching for.</td>
</tr>
</tbody>
</table>

Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boolean</td>
<td>Whether the given path exists in the XML DOM.</td>
</tr>
</tbody>
</table>

POST and URL parameter APIs

POST and URL parameters can be accessed as properties of the `request` object using `request.postParams` and `request.urlParams`.

Any single parameter can be accessed as a property of the `postParams` and `urlParams` parent objects by calling `request.postParams.myParam`. Any parameter accessed this way is an object of the underlying class `ParameterValue`. Any APIs in this class can be called on any parameter.

After inspecting the client request, it may be necessary to access and encrypt parameter values from the request object. Depending on the data in the client request, you can encrypt values and map them to fields on the instance in multiple ways.
Encrypt the value of a known table and field

If you know the name of the instance table and field that will hold the encrypted data, you can explicitly define them in the encryption rule. For example, you may know that the request will be processed on the instance to create an incident and you want to encrypt the text parameter in the description field. In this case, you can create the following action.

```javascript
function SampleAction1() {
    request.postParams.text.valueFor('incident', 'description');
}
```

Encrypt the value of a dynamically defined table and field

If, conversely, you do not know the name of the field that the encrypted data will populate, you can dynamically define them using tableName and fieldName.

The below example processes a generic request that might store data in different task tables (such as incident, problem, and change_request) on the instance.

```javascript
function SampleAction2() {
    var tableName = request.urlParams.table;
    for (var parameter in request.postParams) {
        var currentParam = request.postParams[parameter];
        var fieldName = currentParam.toString();
        if (fieldName == 'text') {
            currentParam.valueFor(tableName, 'description')
        } else {
            currentParam.valueFor(tableName, fieldName);
        }
    }
}
```

This action:
- Gets the destination table from the URL parameters.
- Iterates over the URL parameters.
- Asks the Edge Encryption proxy server to encrypt any URL parameter with a name that matches a field marked for encryption.
- Looks for a specific parameter called text and asks the Edge Encryption proxy to encrypt the value based on the encryption configuration for the description field on the incident table.

In this example, the valueFor() method is not actually performing any encryption. Rather, the method asks the Edge Encryption proxy server to check whether the table/field pair in the request object is marked for encryption with an encryption configuration and, if applicable, encrypt it.

Encrypt JSON or XML within a parameter

A POST or URL parameter might include JSON or XML content. In this case, you can process the content within the parameter, iterate over the values, and encrypt required fields. In this example, the tableName is still accessed from a POST parameter, but the value of the field is the JSON object data.

```javascript
function SampleAction3() {
    var tableName = request.postParams.table;
    var data = request.postParams.data;
    var dataIterator = data.getAsJsonContent().iterator();
```
while (dataIterator.hasNext()) {
    var jsonElement = dataIterator.next();
    var fieldName = jsonElement.getName();
    if (fieldName == 'text') {
        jsonElement.valueFor(tableName, 'description');
    } else {
        jsonElement.valueFor(tableName, fieldName);
    }
}

An example of an encryption rule action that processes XML within a POST parameter.

function SampleAction4() {
    var tableName = request.postParams.table;
    var data = request.postParams.data;
    var dataIterator = data.getAsXmlContent().getIteratorOverAllChildren();
    while (dataIterator.hasNext()) {
        var jsonElement = dataIterator.next();
        var fieldName = jsonElement.getName();
        if (fieldName == 'text') {
            jsonElement.valueFor(tableName, 'description');
        } else {
            jsonElement.valueFor(tableName, fieldName);
        }
    }
}

Encrypt a query

You might encounter an encoded query within a parameter in the client request that contains sensitive data. To match a field in a query to an encrypted value in the instance database, you must create an encryption rule that asks the proxy to check whether a field in the query is marked for encryption. The `encodedQueryFor()` method parses an encoded query on a given table, and checks if any fields in the query have encryption configurations.

In this example, the rule iterates over the parameters looking for the `filter` parameter, which is expected to be a Glide encoded query.

function SampleAction5() {
    var tableName = request.urlParams.table;
    for (var parameter in request.postParams) {
        var currentParam = request.postParams[parameter];
        var fieldName = currentParam.toString();
        if (fieldName == 'filter') {
            currentParam.encodedQueryFor(tableName);
        } else {
            currentParam.valueFor(tableName, fieldName);
        }
    }
}

For example, if the value of `filter` is: `short_description=My sensitive information^number=INC000056^category=Outage`, the query would become `short_description=<Encrypted(My sensitive information)>^number=INC000056^category=Outage` on the instance.
Converts the POST or URL parameter value to a string.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Returns**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>The parameter value as a string.</td>
</tr>
</tbody>
</table>

**ParameterValue - getAsJsonContent()**

Returns the request as an iterable object of type `JsonNode`.

This method is available only in an Edge Encryption rule if the request body is a valid JSON payload. If you are not sure what format the request body includes, check the `contentType` field on the `request` object.

Once the request is returned as a `JsonNode` object, you can use the JSON APIs to iterate over the object and encrypt fields.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Returns**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>JsonNode</td>
<td>The request as an iterable <code>JsonNode</code>.</td>
</tr>
</tbody>
</table>

**ParameterValue - getAsXmlContent()**

Returns the request content as an iterable object of type `XMLContent`.

This method is available only in an Edge Encryption rule. This method assumes that the request body is a valid XML payload. You can check the `contentType` to make sure.

Once the request is returned as an `XMLContent` object, you can use the XML APIs to iterate over the object and encrypt fields.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Returns**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>XMLContent</td>
<td>The request as an iterable object of type <code>XMLContent</code>.</td>
</tr>
</tbody>
</table>
ParameterValue - encodedQueryFor(String tableName)
Specifies that the value of the element is an encoded query on the specified table.

Calling this function on a parameter tells the proxy that the value of the parameter is an encoded query for the specified table. The proxy parses the encoded query and encrypts the fields in the encoded query that must be encrypted.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tableName</td>
<td>String</td>
<td>The table that you expect the query to run on.</td>
</tr>
</tbody>
</table>

**Returns**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>void</td>
<td></td>
</tr>
</tbody>
</table>

ParameterValue - valueFor(String tableName, String fieldName)
Specifies that the value of the element maps to the specified field in the specified table.

Calling this method on an element value tells the proxy that the value for this element maps to the specified field in the specified table. The proxy then checks if the field must be encrypted.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tableName</td>
<td>String</td>
<td>The table name.</td>
</tr>
<tr>
<td>fieldName</td>
<td>String</td>
<td>The field name.</td>
</tr>
</tbody>
</table>

**Returns**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>void</td>
<td></td>
</tr>
</tbody>
</table>

XML APIs
XML APIs can be used after calling getAsXmlContent() on either the request object or a ParameterValue property.

When using XML APIs to write your encryption rule, you can follow a general format:

1. Call getAsXmlContent() on the request object or ParameterValue property. This returns an iterable object of the XMLContent underlying class.

2. Call getIterator() or getIterator(String xPath) on the XMLContent object. This returns an XMLElementIterator object that can be used to iterate over XML elements.

3. Call the hasNext() method on the XMLElementIterator object to determine whether another element is available.

4. Call next() on the XMLElementIterator object to return the next XML element. You cannot call next() without first calling hasNext().
5. Call `valueFor(String tableName, String fieldName)` on the XML element. This method tells the proxy that the value for this element maps to the specified field in the specified table. The proxy then checks if the field must be encrypted.

Note: To determine if you want to call `valueFor(String tableName, String fieldName)` on an XML element, you can use the `getName()` method to return the name of the element.

Mapping to a known table-field on the instance

In this example, the XML payload will be processed on the instance to insert records in the incident table. The description field will populate short_description on the incident.

```
<data>
  <record>
    <name>'Test Record 1'</name>
    <description>'Test Record 1 Description'</description>
    <tag>critical</tag>
  </record>
  <record>
    <name>'Test Record 2'</name>
    <description>'Test Record 2 Description'</description>
    <tag>security</tag>
  </record>
</data>
```

The following encryption rule action can apply:

```
function sampleXmlAction1() {
  var xmlContent = request.getAsXmlContent();
  // This loop iterates over all description tags that match the given path
  var xmlElementIterator = xmlContent.getIterator('data/record/description');
  while (xmlElementIterator.hasNext()) {
    var xmlElement = xmlElementIterator.next();
    xmlElement.valueFor('incident', 'short_description');
  }
}
```

This action iterates through the `description` tags and asks the proxy server to encrypt the values and insert them into `incident.short_description` on the instance.

Note: This rule finds all `description` tags within all `record` tags in the XML payload. If there is only one occurrence of a tag to encrypt, the rule still uses the xPath and iterator structure. However, it iterates only once in the loop.

Mapping to an unknown table-field on the instance

In this example, the rule iterates over the `record` tags, but does not know what tags to expect within the `record` tag. The only known is that the tags within the `record` tags match the names of the columns specified in the table URL parameter.
The rule also specifies that, if the table is incident, then the data in the **description** tag should be encrypted and stored in the **short_description** field on the instance.

```javascript
function sampleXmlAction2() {
    var xmlContent = request.getAsXmlContent();
    var tableName = request.urlParam.table;
    // This first iterator will iterate over all record elements
    var xmlElementIterator = xmlContent.getIterator('data/record');
    while (xmlElementIterator.hasNext()) {
        encryptFieldsInRecord(xmlElementIterator.next());
    }
}

function encryptFieldsInRecord(xmlElement) {
    // Then, iterate over all tags representing fields in the table
    var fieldIterator = xmlElement.getIteratorOverAllChildren();
    while (fieldIterator.hasNext()) {
        var field = fieldIterator.next();
        var fieldName = childElement.getName();
        // If table is incident, then description is encrypted for the
        // short_description field
        if (tableName == 'incident' && fieldName == 'description') {
            field.valueFor(tableName, 'short_description');
        // If table is not incident, ask the proxy to check if the given
        field is encrypted for the given table
        } else {
            field.valueFor(tableName, fieldName);
        }
    }
}
```

In the `encryptFieldsInRecord()` function, the `valueFor()` method is called on a table and a field that are dynamically assigned based on the request. Even though the table and field names can change, the rule asks the proxy to check whether the field in the table must be encrypted based on the encryption configurations defined.

If the field is not configured for encryption, or if the tag does not match a field in the table, the proxy skips that tag. If the tag matches a field marked for encryption, then the Edge Encryption proxy server encrypts the value.

**Using an encoded query**

In this example, all tags have the **filter** attribute, which indicates whether the tag contains an encoded query.

```xml
<data>
    <record>
        <name filter="false">'Test Record 1'</name>
        <description filter="false">'Test Record 1 Description'</description>
        <query filter="true">category=1^name=edge</query>
    </record>
    <record>
        <name filter="false">'Test Record 2'</name>
        <description filter="false">'Test Record 2 Description'</description>
        <query filter="true">category=2^severity=3</query>
    </record>
</data>
```

The following encryption rule action can apply:

```javascript
function sampleXmlAction3() {
    var xmlContent = request.getAsXmlContent();
    var xmlElement = xmlContent.getIterator('data/record');
    while (xmlElement.hasNext()) {
        encryptFieldsInRecord(xmlElement.next());
    }
}
```
var tableName = request.urlParam.table;

// This first iterator will iterate over all record elements
var xmlElementIterator = xmlContent.getIterator('data/record');
while (xmlElementIterator.hasNext()) {
    encryptFieldsInRecord(xmlElementIterator.next());
}
}

function encryptFieldsInRecord(xmlElement) {
    // this time we want to iterate over all tags representing fields in the table
    var fieldIterator = xmlElement.getIteratorOverAllChildren();
    while (fieldIterator.hasNext()) {
        var field = fieldIterator.next();
        var fieldname = childElement.getName();
        // let's look at the filter attribute, if true, then encrypt as encoded query
        if (field.getAttributeValue('filter') == 'true') {
            field.encodedQueryFor(tableName);
        } else {
            // if it is false then check if the field should be encrypted
            field.valueFor(tableName, fieldName);
        }
    }
}

If the filter attribute value is true, the rule asks the proxy server to encrypt the values in the encoded query. If false, the rule asks the proxy to check whether the field should be encrypted.

XMLContent
A global object that provides methods to iterate over the XML content.
You can access an XMLContent object by calling getAsXmlContent() on a request object.

You access XML data in a POST or URL parameter by calling request.postParams.<parameter name>.getAsXmlContent() or request.urlParams.<parameter name>.getAsXmlContent().

XMLContent - getIterator()
Returns an XMLElementIterator object for the XML content.

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>XMLElementIterator</td>
<td>An object that can be used to iterate over elements in the XMLContent object.</td>
</tr>
</tbody>
</table>

XMLContent - getIterator(String xPath)
Returns an XMLElementIterator object for the XML content based on the specified parameter.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>xPath</td>
<td>String</td>
<td>An XPath-like expression that specifies where in the XMLContent object to start.</td>
</tr>
</tbody>
</table>

**Returns**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>XMLElementIterator</td>
<td>An object that can be used to iterate over elements in the XMLContent object.</td>
</tr>
</tbody>
</table>

**XMLElementIterator**

Provides methods for iterating over XML elements.

You get an XMLElementIterator object by calling the `getIterator()` method of the XMLContent class.

**XMLElementIterator - hasNext()**

Determines if there is another element available.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Returns**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boolean</td>
<td>True if another element is available.</td>
</tr>
</tbody>
</table>

**XMLElementIterator - next()**

Returns the next element in the iterator.

You cannot call `next()` without first calling `hasNext()`.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Returns**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>XMLElement</td>
<td>The next XML element.</td>
</tr>
</tbody>
</table>
XMLElement

Provides methods for iterating through XML elements and mapping values to fields in a table.

You get an XMLElement object by calling the next() method of an XMLElementIterator object.

XMLElement - getIterator(String xPath)

Returns an XMLElementIterator object for the XML element based on the specified parameter.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>xPath</td>
<td>String</td>
<td>An xPath-like expression that specifies where in the XMLElement object to start.</td>
</tr>
</tbody>
</table>

Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>XMLElementIterator</td>
<td>An object that can be used to iterate over elements in the XMLElement object.</td>
</tr>
</tbody>
</table>

XMLElement - getIteratorOverAllChildren()

Returns an XMLElementIterator object that includes all sub-elements for the XML element based on the specified parameter.

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>XMLElementIterator</td>
<td>An object that can be used to iterate over elements in the XMLElement object.</td>
</tr>
</tbody>
</table>

XMLElement - valueFor(String tableName, String fieldName)

Specifies that the value of the element maps to the specified field in the specified table.

Calling this method on an element value tells the proxy that the value for this element maps to the specified field in the specified table. The proxy then checks if the field must be encrypted. If the table and field names are unknown, you can call the valueFor() method on a table and a field that are dynamically assigned based on the request.

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tableName</td>
<td>String</td>
<td>The table name.</td>
</tr>
<tr>
<td>fieldName</td>
<td>String</td>
<td>The field name.</td>
</tr>
</tbody>
</table>
XMLElement - encodedQueryFor(String tableName)

Specifies that the value of the element is an encoded query for the specified table.

Calling this function on an element tells the proxy that the value of the element is an encoded query for the specified table. The proxy parses the encoded query and encrypts the fields in the encoded query that must be encrypted.

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tableName</td>
<td>String</td>
<td>The table that you expect the query to run on.</td>
</tr>
</tbody>
</table>

XMLElement - getName()

Returns the element name.

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

XMLElement - getAttributeValue(String attribute)

Returns the value of the specified attribute.

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>attribute</td>
<td>String</td>
<td>Attribute name.</td>
</tr>
</tbody>
</table>
Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>The attribute value.</td>
</tr>
</tbody>
</table>

**JSON APIs**

JSON APIs can be used after calling `getAsJsonContent()` on either the request object or a `ParameterValue` property.

When using JSON APIs to write your encryption rule, you can follow a general format:

1. Call `getAsJsonContent()` on the request object. This returns an iterable object of the `JsonNode` underlying class.
2. Call `getIterator()` or `getIterator(String xPath)` on the `JsonNode` object. This returns a `JsonNodeIterator` object that can be used to iterate over nodes in the JSON object.
3. Call the `hasNext()` method on the `JsonNodeIterator` object to determine whether another element is available.
4. Call `next()` on the `JsonNodeIterator` object to return the next JSON element. You cannot call `next()` without first calling `hasNext()`.
5. Call `valueFor(String tableName, String fieldName)` on the JSON element. This method tells the proxy that the value for this element maps to the specified field in the specified table. The proxy then checks whether the field must be encrypted.

**Note:** To determine if you want to call `valueFor(String tableName, String fieldName)` on a JSON element, you can use the `getName()` method to return the name of the element.

**Mapping to a known table-field on the instance**

In this example, the JSON payload is processed on the instance to insert records in the incident table. The description field populates short_description on the incident.

```json
{
  data: {
    records: [
      {
        "name": "Test Record 1",
        "description": "Test Record 1 Description",
        "tag": "security"
      },
      {
        "name": "Test Record 1",
        "description": "Test Record 1 Description",
        "tag": "security"
      }],
    "query": "assigned_to=3D4860165813e63a00d00abd322244b092^category=vulnerability"
  },
  "source": "10.11.13.14"
}
```
The following rule can apply:

```javascript
function sampleJsonAction1() {
    var jsonContent = request.getAsJsonContent();
    // This loop iterates over all description elements in the records array
    var jsonNodeIterator = jsonContent.getIterator('/data/records/description');
    while (jsonNodeIterator.hasNext()) {
        var jsonNode = jsonNodeIterator.next();
        jsonNode.valueFor('incident', 'short_decription');
    }
}
```

This action iterates through the `description` nodes and asks the proxy server to encrypt the values and insert them into `incident.short_description` on the instance.

**Note:** This rule finds all `description` nodes within the JSON payload. If there is only one occurrence of a node to encrypt, the rule still uses the XPath and iterator structure. However, it iterates only once in the loop.

### Mapping to an unknown table-field on the instance

In this example, the rule iterates over `records`, but is not sure what nodes to expect. The only known is that for each object within `records`, the nodes match the names of the columns specified in the table URL parameter.

The rule also specifies that, if the table is incident, then the data in the `description` node should be encrypted and stored in the `short_description` field on the instance.

```javascript
function sampleJsonAction2() {
    var jsonContent = request.getAsJsonContent();
    var tableName = request.urlParam.table;
    // This first iterator will iterate over all record elements
    var jsonNodeIterator = jsonContent.getIterator('data/records');
    while (jsonNodeIterator.hasNext()) {
        encryptFieldsInRecord(jsonNodeIterator.next());
    }
}

function encryptFieldsInRecord(jsonNode) {
    // this time we want to iterate over all nodes
    var fieldIterator = jsonNode.iterator();
    while (fieldIterator.hasNext()) {
        var field = fieldIterator.next();
        var fieldname = childElement.getName();
        if (fieldname == 'description') {
            field.valueFor(tableName, 'short_description');
        } else {
            field.valueFor(tableName, fieldname);
        }
    }
}
```

In the `encryptFieldsInRecord()` function, the `valueFor()` method is called on a table and a field that are dynamically assigned based on the request. Even though the table and field names can change, the rule asks the proxy to check whether the field in the table must be encrypted based on the encryption configurations defined.

If the field is not configured for encryption, or if the node name does not match a field in the table, the proxy skips that node. If the node name matches a field marked for encryption, then the proxy encrypts the value.
Using an encoded query

```javascript
function sampleJsonAction3() {
    var jsonContent = request.getAsJsonContent();
    var tableName = request.urlParam.table;
    // This first iterator will iterate over all record elements
    var jsonNodeIterator = jsonContent.getIterator('data');
    while (jsonNodeIterator.hasNext()) {
        var jsonNode = jsonNodeIterator.next();
        if (jsonNode.getName() == 'records')
            encryptRecords(jsonNodeIterator.next());
        else if (jsonNode.getName() == 'query')
            jsonNode.encodedQueryFor(tableName);
    }
}
function encryptRecords(jsonNode) {
    //we iterate over all fields in the node
    var recordIterator = jsonNode.iterator();
    while (recordIterator.hasNext()) {
        encryptFieldsInRecord(recordIterator.next());
    }
}
function encryptFieldsInRecord(jsonNode) {
    //this time we want to iterate over all nodes
    var fieldIterator = jsonNode.iterator();
    while (fieldIterator.hasNext()) {
        var field = fieldIterator.next();
        var fieldName = childElement.getName();
        field.valueFor(tableName, fieldName);
    }
}
```

In this example, the rule iterates over `data`. As it finds `records`, it performs the same logic as in the second example, iterating over fields in each node. When it finds the `query` node, it calls `encodedQueryFor()` to encrypt values that should be encrypted in the query.

**JsonNode**

A global object that provides methods to iterate over the JSON content.

You can access a `JsonNode` object by calling `getAsJsonContent()` on a request object.

You access JSON content from a POST or URL parameter by calling `request.postParms.<parameter name>.getAsJsonContent()` or `request.urlParms.<parameter name>.getAsJsonContent()`.

**JsonNode - getIterator(String xPath)**

Returns a `JsonNodeIterator` object for the JSON content.

This method can only be used on the root node, but can be used to traverse deep into the JSON object. Subsequent traversals must use the `iterator()` method.

### Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>xPath</td>
<td>String</td>
<td>An xPath expression.</td>
</tr>
</tbody>
</table>
### Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>JsonNodeIterator</td>
<td>An object that can iterate over nodes in the JSON object.</td>
</tr>
</tbody>
</table>

**JsonNode - iterator()**

Returns a `JsonNodeIterator` object that iterates over all child nodes of the current node.

#### Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Returns**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>JsonNodeIterator</td>
<td>An object that can iterate over nodes in the JSON object.</td>
</tr>
</tbody>
</table>

**JsonNode - getAsString()**

Returns the current node value as a string.

#### Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Returns**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>The current node value.</td>
</tr>
</tbody>
</table>

**JsonNode - getAsString(String propertyName)**

Returns the string value of the specified property.

#### Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>propertyName</td>
<td>String</td>
<td>Name of the property.</td>
</tr>
</tbody>
</table>

**Returns**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>The property value.</td>
</tr>
</tbody>
</table>

**JsonNode - getName()**
Returns the name of the current JSON node.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Returns**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>Name of the current JSON node.</td>
</tr>
</tbody>
</table>

JsonNode - valueFor(String tableName, String fieldName)

Specifies that the JSON property maps to the specified field in the specified table.

Calling this method on a JSON property tells the proxy that the value for this property maps to the specified field in the specified table. The proxy then decides if the field must be encrypted. If the table and field names are unknown, you can call the `valueFor()` method on a table and a field that are dynamically assigned based on the request.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tableName</td>
<td>String</td>
<td>The table name.</td>
</tr>
<tr>
<td>fieldName</td>
<td>String</td>
<td>The field name.</td>
</tr>
</tbody>
</table>

**Returns**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>void</td>
<td></td>
</tr>
</tbody>
</table>

JsonNode - encodedQueryFor(String tableName)

Specifies that the value of the JSON property is an encoded query for the specified table.

Calling this function on a JSON node tells the proxy that the value is an encoded query for the specified table. The proxy parses the encoded query and encrypts the values for fields in the encoded query that must be encrypted.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tableName</td>
<td>String</td>
<td>The table that you expect the query to run on.</td>
</tr>
</tbody>
</table>

**Returns**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>void</td>
<td></td>
</tr>
</tbody>
</table>
JsonNodeIterator

You get a JsonNodeIterator object by calling the getIterator() or iterator() methods of the JsonNode class.

JsonNodeIterator - hasNext()

Determines if there is another property available.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Returns**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boolean</td>
<td>True if another property is available.</td>
</tr>
</tbody>
</table>

JsonNodeIterator - next()

Returns the next property in the iterator.

You cannot call next() without first calling hasNext().

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Returns**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>JsonNode</td>
<td>The next JsonNode.</td>
</tr>
</tbody>
</table>

print(String message)

Prints a message to the wrapper log file: <proxy server directory>/logs/wrapper_<date>.log.

This method is available only in an Edge Encryption rule action script.

**Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>message</td>
<td>String</td>
<td>The message to be written to the wrapper log file.</td>
</tr>
</tbody>
</table>

**Returns**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>void</td>
<td></td>
</tr>
</tbody>
</table>
The Edge Encryption proxy validates encryption rule scripts before saving the rule. Many JavaScript keywords are not allowed in encryption rule scripts.

### Prohibited keywords

<table>
<thead>
<tr>
<th>Keyword</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DIR</strong></td>
</tr>
<tr>
<td><strong>FILE</strong></td>
</tr>
<tr>
<td><strong>LINE</strong></td>
</tr>
<tr>
<td><strong>parent</strong></td>
</tr>
<tr>
<td><strong>proto</strong></td>
</tr>
<tr>
<td>Error</td>
</tr>
<tr>
<td>eval</td>
</tr>
<tr>
<td>getClass</td>
</tr>
<tr>
<td>getPrototypeOf</td>
</tr>
<tr>
<td>Java</td>
</tr>
<tr>
<td>javax</td>
</tr>
<tr>
<td>javafx</td>
</tr>
<tr>
<td>JavaImporter</td>
</tr>
<tr>
<td>load</td>
</tr>
<tr>
<td>loadWithNewGlobal</td>
</tr>
<tr>
<td>new</td>
</tr>
<tr>
<td>Packages</td>
</tr>
<tr>
<td>Object</td>
</tr>
<tr>
<td>prototype</td>
</tr>
<tr>
<td>RegExp</td>
</tr>
<tr>
<td>setPrototypeOf</td>
</tr>
<tr>
<td>this</td>
</tr>
<tr>
<td>throw</td>
</tr>
</tbody>
</table>

### Edge Encryption dictionary attributes

You can add Edge Encryption dictionary attributes to tables and fields.

To set an Edge Encryption dictionary attribute to true, you must enter `attribute=true` in the **Attributes** field.

To add a dictionary attribute to a record, see [Dictionary attributes](#).

**Edge Encryption Excluded [edge_encryption_excluded]**

When set to true, the field or table cannot be encrypted.

- Value: true/false
- Target element: field or table
• Default value: false

**Edge Encryption Enabled [edge_encryption_enabled]**

When set to true, the field is eligible for encryption through an encryption configuration. Because this attribute is used by the system and cannot be modified, it is not always displayed to the user.

*Note:* This attribute does not indicate that a field is encrypted, nor does it trigger any encryption logic on the field. Rather, the attribute determines the possibility of the field being encrypted by a user.

• Value: true/false
• Target element: field
• Default value: true for String fields

**Edge Encryption Clear Text Allowed [edge_encryption_clear_text_allowed]**

When set to true, allows server-side scripts to append non-encrypted data to an encrypted string within the field for user actions performed through the proxy server, or any server-side automated scripts, such as scheduled jobs.

• Value: true/false
• Target element: field
• Default value: false

**Domain separation and Edge Encryption**

Domain separation is unsupported in Edge Encryption. This application provides the ability to encrypt data from within the customer's environment through the use of specific configurations, rules, and keys defined on the Edge Encryption proxy. The Edge Encryption proxy is not domain aware and cannot support domain-specific settings. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can control several aspects of this separation, including which users can see and access data.

**Support level: No support**

• The domain field may exist on data tables but there is no business logic to manage the data.
• This level is not considered domain-separated.

For more information, see Application support for domain separation.

**How domain separation works in Edge Encryption**

Edge Encryption can be used where domain-specific keys, configurations, and rules are not required.

*Note:* It is not recommended to install Edge Encryption on domain instances at all even for internal service provider usage.

**Data integration with Edge Encryption**

To integrate third-party data with an instance using Edge Encryption, you must route the data through the Edge Encryption proxy server using supported integrations. Supported integrations use base system encryption rules that map data in each payload to fields in a table.
Upload data to fields marked for encryption

Edge Encryption does not support importing data from or exporting data to Excel, CSV, XML, or other file types to or from fields with encryption configurations defined.

**ODBC driver**

Encrypt requests and query data through the Edge Encryption proxy server using the ODBC driver.

Learn more: [Edge Encryption ODBC driver integration](#)

**MID Server**

You can configure the MID Server to route data through an Edge Encryption proxy server. However, some restrictions apply.

Learn more: [Edge Encryption MID Server integration](#)

**REST/SOAP web services**

Use REST/SOAP web services to update or retrieve record data through the Edge Encryption proxy server.

Learn more: [Web services](#)

**JSONv2 web service**

Use JSONv2 web service APIs to update or retrieve record data through the Edge Encryption proxy server. Base system encryption rules support data retrieval and data modification APIs.

- To insert a single record using the data modification API, use the `insert()` or `insertMultiple()` methods.
- To insert multiple records using the data modification API, use the `insertMultiple()` method.

Learn more: [JSONv2 Web Service](#)

To encrypt data from custom third-party integrations not listed above, create custom encryption rules. See [Define a custom encryption rule](#).

Upload attachments to records marked for encryption

Attachments can be uploaded to tables with attachment encryption configured using REST and SOAP web services.

**Edge Encryption ODBC driver integration**

Configure your ODBC driver to query data encrypted by Edge Encryption. The Edge Encryption proxy server encrypts ODBC driver requests to the ServiceNow instance when Edge Encryption is integrated with the ODBC driver.

Encrypted responses from the instance are decrypted through the Edge Encryption proxy server before passing to the ODBC driver in your network.
For a successful integration, the ODBC driver must trust the Edge Encryption proxy server certificate. If the Edge Encryption proxy server certificate is signed by a Certificate Authority trusted by the ODBC driver, the Edge Encryption proxy server is automatically trusted. However, if a Certificate Authority trusted by the ODBC driver has not signed the Edge Encryption proxy server certificate, you must import the self-signed certificate to the ODBC truststore.

Import a self-signed certificate to the ODBC truststore
If a Certificate Authority trusted by the ODBC driver has not signed the Edge Encryption proxy server certificate, you must import a self-signed certificate to the ODBC truststore. You can export the certificate from the Edge Encryption proxy server and import it into the ODBC truststore.

To determine whether a Certificate Authority trusted by the ODBC driver has signed the Edge Encryption proxy server certificate, run the following command in the keystore directory in the proxy home directory to view a list of Certificate Authorities trusted by the ODBC driver:

```
keytool -keystore "<ODBC directory>\ip\Java\jre\lib\security\cacerts" -list
```

1. Change to the keystore directory in the proxy home directory.
2. Check the keystore for the self-signed certificate.
   a) To check the keystore for the certificate, you can run the following command to list all the items in the keystore.

```
keytool -list -keystore keystore.jceks -storetype jceks -v
```
   b) Locate the key alias in the list of items.
3. Using the key alias, export the certificate to a .cer file.

```
keytool -export -alias <key alias> -keystore keystore.jceks -storetype jceks -rfc -file <file name>.cer
```
4. Change to your ODBC truststore directory: ODBC\ip\Java\jre\lib\security\cacerts.
5. Import the certificate to your ODBC truststore.

```
keytool -keystore cacerts -importcert -alias $<key alias> -file <file name>.cer
```

Set the ODBC driver properties

Set the ODBC driver properties to route requests through the Edge Encryption proxy server.

1. In Windows, navigate to Start > Programs > ServiceNow ODBC Management Console.
2. Expand the console tree root to: ServiceNow ODBC Manager\Manager\<installation location>\Services\ServiceNow_ODBC\Data Source Settings\ServiceNow\IP Parameters.
3. Double-click the DataSourceIPProperties attribute.
4. Change the **Value** to the URL of your Edge Encryption proxy server, such as `https://<IP address>:<port>`
5. Click OK.

The ODBC driver is now configured to route requests to the instance through the Edge Encryption proxy server.

**Edge Encryption MID Server integration**

Configure the MID Server to route data through an Edge Encryption proxy server.

When integrated with the MID Server, the Edge Encryption proxy server acts as the MID Server’s endpoint. The Edge Encryption proxy server then encrypts and decrypts data passing between the ServiceNow instance and the MID Server.

**Limitations when integrating with the MID Server**

When MID Server data is configured to pass through the Edge Encryption proxy server, the following limitations apply:

- Encryption of ECC Queue fields is not supported.
- Encrypted data cannot be used with Discovery or Service Mapping.

**Point the MID Server to the Edge Encryption proxy server**

To pass data from the MID Server through the Edge Encryption proxy server, update the MID Server configuration file to point the MID Server to the Edge Encryption proxy server.

When configuring the MID Server to pass through the Edge Encryption proxy server, you cannot use the web proxy properties in the MID Server configuration file to route traffic through the Edge Encryption proxy server to your instance. Instead, you must set the Edge Encryption proxy server as the MID Server’s endpoint.

1. Navigate to your local MID Server directory and open the `config.xml` file.
2. Find the element `<parameter name="url" value="https://YOUR_INSTANCE.service-now.com" />` and change the value property to the URL of your Edge Encryption proxy server. For example, `http://hostname.mycompany.com:8081`.
   This step directs the MID Server to pass traffic to the Edge Encryption proxy server instead of the instance. The Edge Encryption proxy server in turn encrypts any necessary fields and passes the payload to the instance.
3. Save and close the file.
4. If running, restart the MID Server.

**Edge Encryption diagnostics and performance**

Monitor Edge Encryption proxy server performance trends and drill into errors generated by the Edge Encryption proxy server.

### Edge proxy performance

View key Edge Encryption proxy server performance trends using the Edge Proxy graph set on the ServiceNow Performance homepage. Monitored trends include:

- Maximum and average response times between the client, proxy server, and instance.
- CPU, disk space, and memory usage of the host machine.
- Maximum and average network latency between the proxy server and the ServiceNow instance.

**Note:** Edge Encryption proxy servers with duplicate names do not report performance trends.
Graph Set

Monitorable Items

Edge Proxy

Proxy Server

Edge Processing (Max)

Processing Time (Ms)

0 250 500 750 1000

15:20 15:30 15:40 15:50

Total Time  Proxy Response  Proxy–Instance Round Trip

Edge Processing (Average)

Processing Time (Ms)

0 200 400 600

15:20 15:30 15:40 15:50

Total Time  Proxy Response  Proxy–Instance Round Trip

Edge Proxy Performance (Max)

Percent

0 50 100 150

15:20 15:30 15:40 15:50

CPU Usage  Memory Usage  Disk Usage

Edge Proxy Performance (Average)
Maximum and average time in milliseconds to process a request. These data points are general trends over time.

- **Total Time**: Time for the proxy server to receive a request from a client and send a response. This data point is the sum of the subsequent data points.
- **Proxy Response**: Time for the proxy server to process a response from the instance.
- **Proxy-Instance Round Trip**: Time for the proxy server to send a request to the instance and receive a response. Includes network latency between the proxy server and the instance and time spent by the instance to process the request.
- **Rules**: Time for the proxy server to evaluate a request using defined encryption rules.
- **Proxy Request**: Time for the proxy server to process a client request and forward it to the instance.

**Edge Proxy Performance (Max and Average)**

Maximum and average percentage of resources used on the host machine.

- CPU Usage
- Memory Usage
- Disk Usage

**Edge Proxy Latency**

Maximum and average network latency in milliseconds at a given point in time. Latency is determined by round-trip time for a proxy server to send a simple ping to the instance and receive a response.

**Proxy Error Reports**

Navigate to **Edge Encryption Configuration > Diagnostics and Troubleshooting > Proxy Error Reports** to view all proxy server errors collected over the past seven days.
Errors are collected over a one-minute period. Each minute, an error report is generated. The vertical axis displays the number of error reports over the last seven days that include each error. For example, even if the DEFAULT_ERROR_CODE error is thrown multiple times over a one-minute report period, the DEFAULT_ERROR_CODE bar will only reach one on the **Number of Error Reports** axis.

From this view, you can:

- Click each proxy error code bar to see the report on a single error for each proxy server. From this view, you can click the bar again to view the error text in the Edge Encryption Proxy Stat table [edge_encryption_stat]. Follow links in the error text to see more information and possible remediation steps.
- Click **Other** to see page two of the error report.

**Note:** If you have more than one proxy server with the same name, a single DUPLICATE_PROXY_NAME error appears in the Proxy Error Report. No other errors are reported for proxy servers with duplicate names. If you encounter this error, make sure that all proxy servers have unique names.

### Additional monitoring resources

The instance tracks all encryption proxies. Each Edge Encryption proxy server registers when it starts up. The instance is notified when:

- A new Edge Encryption proxy server starts up.
- An Edge Encryption proxy server is intentionally shut down.

If an Edge Encryption proxy server attempts to register with an instance that does not have Edge Encryption installed, the proxy does not start.
All encryption configuration files are audited. Deleted records are audited on all encryption configuration files. Audit records are put in the sys_audit table. To view the history of a specific configuration record, view the record, and click History > List in the menu. The Mass Encryption Job is not audited.

Use the following additional resources to monitor you proxy servers.

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid Insert Attempts</td>
<td>List of attempts to save the following data to encrypted fields:</td>
</tr>
</tbody>
</table>
| [sys_edge_encryption_invalid_insert_log] | • Unencrypted data.  
|                                | • Data that did not come from an Edge Encryption proxy.                       |
|                               | The instance rejects and then logs any attempts to save this data. If you have the security-admin role, you can view the logs in the Invalid Insert Attempts list. |
| Job Failures                  | A list of jobs that did not execute successfully.                           |
| [sys_encryption_job_execution] |                                                                             |
| System logs                   | The instance periodically checks for messages from each registered proxy server. If a proxy server has not sent a message in the required time frame, an error is logged. The log message contains information about the encryption proxy and the last time the proxy pinged the instance. If the instance determines that none of the encryption proxies are online, it logs a message. These messages are added to the system log. |

**Disable or reduce Edge Proxy statistic collection**

Prevent the Edge Encryption proxy server from sending Edge Proxy Graph Set statistics to the ServiceNow Performance homepage, or reduce the frequency of statistic collection.

Role required: admin or security_admin

By adding properties in the edgeencryption.properties configuration file, you can:

- Disable the Edge Proxy graph set.
- Change the interval during which statistics are collected by the Edge Encryption proxy server. By default, statistics are collected every 30 seconds.

1. In your proxy server installation directory, open the edgeencryption.properties configuration file located in the <installation directory>/conf/ folder.
2. Add one of the Edge Encryption proxy server properties.
3. Restart the proxy server.

**Data Classification**

Group data by type, using pre-defined or user-defined data classifications. If you have an assigned data classification administrator or auditor role, you can administer different data classes or visually analyze the current state of different types of data within the instance.

Data Classification enables support for:

- Visibility into the types of data hosted on a Now Platform instances.
- Compliance with privacy laws, and meeting regulation requirements for industries such as financial services and medical device manufacturing.
Data classifications

Data classification is a standalone process in which you manually apply data classifications to existing dictionary entries in any table.

- You classify data as you find appropriate for your business and you can alter the available data classes as necessary.
- When you classify data, you can use the pre-defined data classifications, or create your own. Although use of pre-defined data classifications is optional, it is advisable do so as a starting point. These pre-defined data classifications are included in demo data that you can install in your instance. To learn more, see Install Data Classification plugin demo data and Components installed with Data Classification demo data.
- If you create your own data classifications, you can also design a tiered hierarchical system with parent and child data classifications.

Overview dashboard

Use the Overview dashboard to understand how your current data tables map to different data classifications. You can also analyze how your global, regional, international users may require different approaches to data classification, regarding the use or access to data. You can also customize the Overview dashboard content and layout to fit your needs.

To learn how to use the available scripted and REST APIs to apply the classification metadata within existing processes, workflows, and applications, see the following:

- Data Classification - REST API
- DCManager - Global
- ScopedDCManager - Scoped

Note: Data Classification supports domain separation, and the data_classification table itself is process separated.

Use cases

General Data Protection Regulation (GDPR) is a European Union regulation whose purpose is to provide individuals with control over their own personal data. You can use data classifications, such as Personally Identifiable Information, to identify where personal data is being stored in your instance. By applying the appropriate security mechanisms to protect that personal data from leaking out, your organization satisfies GDPR requirements.

If you store customer information in the Now Platform, use the Personally Identifiable Information (PII) classification code where needed to track data subject to regulation by local privacy laws. When you install demo data, it automatically applies this classification code to certain security-sensitive fields in the User [sys_user] table. To learn more, see:

- Components installed with Data Classification demo data
- Assign data classifications to dictionary entries

You can apply a Restricted data classification to Employee table columns that store sensitive employee information such as Social Security Numbers (SSN). Administrators and auditors can then use the Overview dashboard to confirm
that you have assigned data classifications to the correct columns. They can also view the classification details for restricted types of information.

**Install Data Classification plugin demo data**

When you upgrade to or install Quebec (and above), the Data Classification (com.glide.data_classification) plugin is automatically activated. However, you should manually install the demo data that comes with the plugin. It includes several important pre-defined data classifications, and it also assigns one of them to specific User [sys_user] table columns in your instance.

Role required: admin

Regardless of whether you install demo data, the activated Data Classification plugin adds the following user roles in your instance:

- **data_classification_admin**: Can administer all aspects of the Data Classification application, including data classification setup and assignment.
- **data_classification_auditor**: Can audit Data Classification code assignments made to user tables and columns.

1. Navigate to **System Applications > All Available Applications > All**.
2. Find the Data Classification plugin using the filter criteria and search bar.
   - An Installed message appears after you locate the plugin.
3. Click the icon with three vertical dots, then select **Repair** to access the Activate Plugin dialog.

   ![Activate Plugin dialog](image)

   The following dialog box appears:

   ![Activate Plugin dialog contents](image)

4. Select **Load demo data**, and then click **Repair**.
Components installed with Data Classification demo data

When you install the demo data included in the Data Classification (com.glide.data_classification) plugin, several types of components are installed in your instance. These components include pre-defined data classifications and code assignments for specific User [sys_user] columns.

Data Classifications installed

<table>
<thead>
<tr>
<th>Data Classification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidential</td>
<td>Sensitive data that if compromised could negatively affect operations.</td>
</tr>
<tr>
<td>Internal</td>
<td>Internal data not meant for public disclosure.</td>
</tr>
<tr>
<td>Personally Identifiable Information</td>
<td>Also known as PII. Data that could potentially be used to identify a particular person.</td>
</tr>
<tr>
<td>Public</td>
<td>Data that may be freely disclosed to the public.</td>
</tr>
<tr>
<td>Restricted</td>
<td>Highly sensitive corporate data that if compromised could put the organization at financial or legal risk.</td>
</tr>
</tbody>
</table>

Data Classification assignments

<table>
<thead>
<tr>
<th>Table</th>
<th>Assigned Column</th>
<th>Assigned data classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>sys_user</td>
<td>zip</td>
<td>Personally identifiable information</td>
</tr>
<tr>
<td>sys_user</td>
<td>first_name</td>
<td>Personally identifiable information</td>
</tr>
<tr>
<td>sys_user</td>
<td>email</td>
<td>Personally identifiable information</td>
</tr>
<tr>
<td>sys_user</td>
<td>city</td>
<td>Personally identifiable information</td>
</tr>
<tr>
<td>sys_user</td>
<td>middle_name</td>
<td>Personally identifiable information</td>
</tr>
<tr>
<td>sys_user</td>
<td>street</td>
<td>Personally identifiable information</td>
</tr>
<tr>
<td>sys_user</td>
<td>mobile_phone</td>
<td>Personally identifiable information</td>
</tr>
<tr>
<td>sys_user</td>
<td>last_name</td>
<td>Personally identifiable information</td>
</tr>
<tr>
<td>sys_user</td>
<td>country</td>
<td>Personally identifiable information</td>
</tr>
<tr>
<td>sys_user</td>
<td>gender</td>
<td>Personally identifiable information</td>
</tr>
<tr>
<td>sys_user</td>
<td>name</td>
<td>Personally identifiable information</td>
</tr>
<tr>
<td>sys_user</td>
<td>photo</td>
<td>Personally identifiable information</td>
</tr>
<tr>
<td>sys_user</td>
<td>state</td>
<td>Personally identifiable information</td>
</tr>
<tr>
<td>sys_user</td>
<td>home_phone</td>
<td>Personally identifiable information</td>
</tr>
</tbody>
</table>
Create data classifications

Create your own user-defined data classifications in the Data Classification [data_classification] table that you can then assign to specific columns in specific tables.

Role required: data_classification_admin, admin

1. Navigate to System Security > Data classification > Data classes.
2. Fill in the fields on the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classification Name</td>
<td>Name of the data classification.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the data classification.</td>
</tr>
<tr>
<td>Parent</td>
<td>Name of the parent data classification that this data classification is subordinate to. Leave the field empty if this data classification is not a parent to child data classifications.</td>
</tr>
<tr>
<td>Application</td>
<td>Application scope for this data classification.</td>
</tr>
</tbody>
</table>

3. If this data classification should be a parent to child data classifications, click New.

   If you do not want to create child data classifications, skip this step.
4. Fill in the fields on the form.

<table>
<thead>
<tr>
<th>Title</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Classification Name</td>
<td>Name of the child data classification.</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Description of the child data classification.</td>
</tr>
<tr>
<td></td>
<td>Parent</td>
<td>Name of the parent data classification that this data classification is subordinate to. Leave the field empty if this data classification is not a parent to child data classifications.</td>
</tr>
<tr>
<td></td>
<td>Application</td>
<td>Application scope for this child data classification.</td>
</tr>
</tbody>
</table>

5. Click Submit.

Assign data classifications to dictionary entries

Assign data classifications to specific table columns in the Dictionary [sys_dictionary] table. When you assign data classifications, it creates entries in the Dictionary-Data Class [m2m_dictionary_dataclass] table, which you can then review in the Overview dashboard.

Role required: data_classification_admin, admin

1. In the Navigator pane, type sys_dictionary.list.
2. In Dictionary Entries, select each of the elements you want to assign specific data classifications to.
3. After selecting the elements, click Actions on selected rows, and then select Classify.

   Note: To clear previously assigned data classifications for selected dictionary elements, you can select Clear classification.
4. When the Assign to data class dialog appears, select the data classifications you want to assign to your selected dictionary elements, then click **Classify**.

You can select multiple data classifications as needed.

**Analyze data classifications using the Overview dashboard**

The Overview dashboard reports the current state of data classifications within your instance, and how your users are distributed by location. If you have a data classification administrator or auditor role, you can visualize the current sensitivity of instance data, which helps increase security and compliance with privacy laws. By using the Location field in user records, administrators map users across different regions that have differing privacy regulations.
Tables and columns tab

Breakdown of classified data

- Personally identifiable information = 14 (77.78%)
- Internal = 2 (11.11%)
- Confidential = 1 (5.56%)
- Restricted = 1
Users tab

Number of locations

Users by country
Required Now Platform roles

- data_classification_admin: Administers all aspects of the Data Classification application, including data classification setup, and assignment.
- data_classification_auditor: Audits Data Classification code assignments.

Use cases

For additional examples of how different people in your organization would use this dashboard, see Use Cases in Data Classification.

<table>
<thead>
<tr>
<th>User</th>
<th>Dashboard use</th>
</tr>
</thead>
<tbody>
<tr>
<td>data_classification_admin</td>
<td>Confirm that you have assigned data classifications to the correct fields in your instance.</td>
</tr>
<tr>
<td>data_classification_auditor</td>
<td>Audit the senility and security of data in your instance.</td>
</tr>
</tbody>
</table>

Reports

<table>
<thead>
<tr>
<th>Title</th>
<th>Type</th>
<th>Source table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Breakdown of classified data</td>
<td>Pie Chart</td>
<td>m2m_dictionary_dataclass</td>
<td>Provides a breakdown of instance data classifications, by data class.</td>
</tr>
<tr>
<td>Total number of tables</td>
<td>Single Score</td>
<td>sys_dictionary</td>
<td>Total number of data tables in your instance.</td>
</tr>
<tr>
<td>Total number of columns</td>
<td>Single Score</td>
<td>sys_dictionary</td>
<td>Total number of classified data columns in your instance. This count is the number of columns you assigned data classifications to.</td>
</tr>
<tr>
<td>Classified Items Count</td>
<td>Single Score</td>
<td>m2m_dictionary_dataclass</td>
<td>Total number of tables that have been assigned data classifications.</td>
</tr>
<tr>
<td>Number of tables with user reference</td>
<td>Single Score</td>
<td>sys_dictionary</td>
<td>Total number of tables that have at least one column that references the sys_user table.</td>
</tr>
<tr>
<td>Number of locations</td>
<td>Single Score</td>
<td>sys_dictionary</td>
<td>Total number of locations in your instance.</td>
</tr>
<tr>
<td>Number of users</td>
<td>Single Score</td>
<td>sys_user</td>
<td>Total number of users in your instance.</td>
</tr>
<tr>
<td>Users by country</td>
<td>Map</td>
<td>sys_user</td>
<td>Location breakdown of users by country.</td>
</tr>
</tbody>
</table>
Domain separation and Data Classification

Domain separation is supported for Data Classification. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can control several aspects of this separation, including which users can see and access data.

Support level: Enhanced

- Includes Basic and Standard levels
- Data-driven process enables service provider customers to modify business logic that is based on defined use cases. These configurations are UI-based and fail-safe so that configurations by one customer cannot affect another.
- Tenants of the instance must be able to configure minimum viable product (MVP) business logic and data parameters for themselves. This logic and parameters would be expected for the application's normal function.

Use case: Tenant-customers of a shared environment must be able to modify the impact, urgency, or priority matrix to set priority within their domain.

To learn more, see Application support for domain separation.

How domain separation works in Data Classification

For domain separation, the application uses process separation for the Data Classification [sys_data_classification] table. For the Dictionary-Data Class [m2m_dictionary_dataclass] table, it uses data separation. For learn more about data and process separation, see Domain separation explained.

Auditing

Track record changes on auditing-enabled tables. By default, the system tracks changes to the incident, change, and problem tables, among others.

Enabling auditing tracks the creation, update, and deletion of all records in the table. If you want to audit individual fields in a table, you can hide fields you do not want to track using a dictionary attribute.

Auditing information is kept in these tables:
- The Audit table.
- The History sets table.

CAUTION: Auditing certain system tables that receive a large amount of traffic, such as Workflow Contexts [wf_context], can impact performance and is not recommended. The em_alert table itself can have audit=true, but the fields are not audited unless you explicitly set audit=true for a field.

Auditing parent and child tables

Tables do not derive the audit flags from parent or child audited tables.
- For example, if you enable auditing for the cmdb_ci table, only CIs stored in that base table are audited.
- Likewise, if you enable auditing for the cmdb_ci_computer table, only the computer CI records are audited, including any fields on the cmdb_ci_computer table that are derived from the cmdb_ci table.
Auditing system tables

By default, the system does not audit the deletion of a record from system tables. To audit a system table, add it to the list of tables in the glide.ui.audit_deleted_tables property list.

Auditing deletions from a form or list

By default, the system audits deletions of individual records from a form. To prevent auditing, set the table's dictionary attribute no_audit_delete.

The system audits deletions from a list when audit is selected on the table dictionary, and the table is not listed in the glide.db.audit.ignore.delete property.

Note: By default, the glide.db.audit.ignore.delete property is not present in the System Property [sys_properties] table. To change the property, and its associated values, you must first manually add it. However, when manually added, it overwrites the following default values:

```plaintext
glide.db.audit.ignore.delete =
  sys_mutex, sys_db_cache, sys_lucene_block, sys_lucene_file, sys_lucene_directory, sys_user_preference,
  cmdb_ci_windows_service, cmdb_sam_sw_install, cmdb_software_instance,
  cmdb_sam_sw_usage, sam_sw_counter_detail
```

To learn more about adding system properties, see Add a system property.

Information audited

Auditing tracks the following record changes:

- Unique Record Identifier (sys_id) of the record that changed
- Field that changed
- New field value
- Old field value
- Number of times this record and field have been updated
- Date and time when the change occurred
- User who made the change
- Reason for the change (if any reason is associated with the change)
- Internal checkpoint ID for the record, if the record has multiple versions.

Information exempted from auditing

Some updates are not audited despite enabling auditing on a table. It is why you may see 132 updates in a record's history, but only seven audited ones.

Auditing excludes the following information:

- Updates made by an upgrade.
- Updates made through import sets.
- Records in parent or child tables.
- Fields with the no_audit dictionary attribute.
- System tables not listed in the glide.ui.audit_deleted_tables property list.
- Fields that begin with the sys_ prefix (system fields), except the sys_class_name and sys_domain_id columns.
- UI Pages can sometimes trigger updates to a record without creating an audit log.
Anytime an inactivity monitor touches a record. It prevents you seeing possibly hundreds of updates listed against an incident, with the noise drowning out the useful data.

**Auditing a table**

For instructions on how to audit a table, see Enable auditing for a table.

By default, the system tracks all fields in an audited table. You can audit a subset of fields in a table in one of two ways:

- You can enable auditing for the entire table, then exclude those fields you do not want to include. It is appropriate when you want to audit most, but not all, fields, and is referred to as an **exclusion listing**. For more information, see Include a field from being audited (exclusion listing).
- You can enable auditing for the table, but only for specified fields. It is appropriate when you want to audit only a small number of the table’s fields and is referred to as **inclusion listing**. For information on how to include a field using inclusion listing, see Include a table field in auditing (inclusion listing).

**Sys Audit and Audit Relationship Change tables**

The Now Platform tracks inserts and updates to audited records in the Sys Audit (sys_audit) and Audit Relationship Change (sys_audit_relation) tables.

The Now Platform tracks audit tables. To track tables, select the **Audit** check box in the dictionary record to set the value to true. By default, it does not audit records from system tables, such as update sets tables.

**Note:** To prevent performance issues and infinite loops, the system skips any business rule or workflow triggered by inserts to the Sys Audit table.

**Sys audit table columns**

The following columns appear in the sys_audit table records:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table name</td>
<td>Table that the audit record is for (for example, &quot;incident&quot;)</td>
</tr>
<tr>
<td>Field name</td>
<td>Column in the table that the audit record is for (for example, &quot;assigned_to&quot;)</td>
</tr>
<tr>
<td>Document key</td>
<td>Sys_id (Unique Record Identifier) for the originating record associated with the audit record.</td>
</tr>
<tr>
<td>Old value</td>
<td>Old value of the field change represented by this sys_audit record.</td>
</tr>
<tr>
<td></td>
<td>• Reference fields: Unique sys_id value of the changed record.</td>
</tr>
<tr>
<td></td>
<td>• Date and time fields: Value in Coordinated Universal Time (UTC) as stored in the database.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>New value</td>
<td>New value of the field change represented by this sys_audit record.</td>
</tr>
<tr>
<td></td>
<td>• Reference fields: Unique sys_id value of the changed record.</td>
</tr>
<tr>
<td></td>
<td>• Date and time fields: Value in Coordinated Universal Time (UTC) as stored in the database.</td>
</tr>
</tbody>
</table>

How the Audit Relationship Change (sys_audit_relation) table works

The Sys Audit [sys_audit] table tracks activity in tables that are flagged for auditing. This activity includes journal field entries and history sets. The Audit Relationship Change [sys_audit_relation] table tracks relationship changes between sys_audit table records and the source tables that the audited records originate from. It also tracks when a record might have been deleted.

• Whenever you audit any record in a table, a relationship is created between the various originating tables to the store that records data. This relationship information is saved in the sys_history_set, sys_history_line, and sys_journal tables.
• If you delete a field that is related to an audited table record, the sys_audit_relation table records the deletion. In other words, anytime you change an audited record, it first deletes past elements, and then creates a relationship in the sys_audit_relation table with new document IDs.

Enable auditing for a table

You can enable table auditing to track changes to all or some of the table's fields.

Role required: admin

1. Navigate to System Definition > Dictionary.
   The system displays the list of dictionary entries. The list includes a row for each table as well as a row for each column (field) in the table.
2. In the list of dictionary entries, find the row corresponding to the table you want to audit, for example cmdb_ci_computer. You can distinguish the row for the table itself – versus a row for a column in the table – by finding the row with the correct table name, an empty entry for Column name, and a Type of Collection.
3. Select the dictionary entry for the table.
   The system displays the dictionary entry form.
4. Check the Audit check box.
5. Click Update.

If you want to audit only a few fields in the table Enable inclusion list auditing for a table. If you want to audit most – but exclude some – fields, Exclude a field from being audited (exclusion listing).

Enable inclusion list auditing for a table

Enable a table to audit only those fields you explicitly designate. This is useful when you want to audit only a small number of fields in an audited table.

Role required: admin

The table must be enabled for auditing.

1. Navigate to System Definition > Dictionary.
The system displays the list of dictionary entries. The list includes a row for each table as well as a row for each column (field) in the table.

2. If necessary, customize the list view to show the Attributes column.

3. In the list of dictionary entries, find the row corresponding to the table you want to audit, for example cmdb_ci_computer. You can distinguish the row for the table itself – versus a row for a column in the table – by finding the row with the correct table name, an empty entry for Column name, and a type of collection.

4. In the Attributes field for that row, enter audit_type=whitelist.

Designate which fields you want to audit in this table.

**Exclude a field from being audited (exclusion listing)**

Prevent the Now Platform from tracking a subset of fields in an audited table by excluding those fields from an audit.

Role required: admin

To exclude a field in a table from being audited, you must have first enable auditing for that table.

Add a set of fields to an exclusion list when you want to audit most of the fields in an auditable table. If you want to audit only a few fields, follow the inclusion listing procedure instead.

**Note:** Disabling auditing on journal-based fields can impact the functionality of features, such as the Activity Formatter. For more information, see KB0743142.

1. Navigate to System Definition > Dictionary.
2. If necessary, customize the list view to show the Attributes column.
3. Navigate to the row corresponding to the table and field (column) you want to exclude from auditing.
4. In the Attributes column for that row, enter no_audit.

**Include a table field in auditing (inclusion listing)**

Track a subset of fields in an audited table by add those fields to an inclusion listing.

Role required: admin

To add fields in a table to an inclusion list, you must have first enabled auditing for that table and enabled inclusion list auditing for that table.

Add a set of fields to an inclusion list when you want to audit only a small number of an audited table’s fields. If you need to audit most fields, and exclude only a few, follow the exclusion list procedure instead.

1. Navigate to System Definition > Dictionary.
2. If necessary, customize the list view to include showing the Attributes column.
3. Navigate to the table and field (column) you want to the inclusion list.
4. In the Attributes field, enter audit=true.

**Enable auditing for a system table**

Deletions from tables with a sys_ prefix are not audited by default. To track deletions from these tables, add the table name to the glide.ui.audit_deleted_tables property. Enabling the Restore Deleted Records plugin adds several default values to this property.

Role required: admin

1. Navigate to System Properties > UI Properties.
2. Locate the List of system tables (beginning with "sys_", comma separated) that will have the delete audited property.
3. Add or remove table names. Table names should be separated by commas, without any spaces.
4. Click **Save**.

**Note:** For more information about auditing, see Understanding the sys audit Table.

### History sets

The system automatically generates History Set records as needed from the Audit table when a user either creates a record or views its history.

If a record is in an audited table, its history set is generated when the record is inserted or when a user views the record.

**Note:** Do not use history sets to generate reports.

Several fields of information are captured in the History Set record, displayed in the list view.

<table>
<thead>
<tr>
<th>Field</th>
<th>Input Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>List View Record Fields</strong></td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Document ID for the record whose history is being recorded.</td>
</tr>
<tr>
<td>Table</td>
<td>Audited table for the record whose history is being recorded.</td>
</tr>
<tr>
<td>Load Time</td>
<td>Amount of time it took to generate the history set.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Input Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Audit History Record Fields</strong></td>
<td></td>
</tr>
<tr>
<td>Label</td>
<td>Label of the field that was changed.</td>
</tr>
<tr>
<td>Old</td>
<td>Value before the change.</td>
</tr>
<tr>
<td>New</td>
<td>Value after the change.</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates if the entry is for a normal field, an email record, or a relationship change record.</td>
</tr>
<tr>
<td>Update Number</td>
<td>Number of times this field has been changed. A value of -1 indicates when the record was created or deleted.</td>
</tr>
</tbody>
</table>
### History Sets in a Calendar View

Once History Sets are active, the History context menu choice populates using information from the history set, rather than from the `sys_audit` table. From the user's perspective, the same historical data is available in the same user interface, but how the information is stored is different.

Since the History view includes a calendar view, but does not use the normal list interface to filter and interact with the history records, it allows:

- Searching and filtering historic data.
- Exporting historic data.

### Viewing history sets

There are two ways of viewing the history set, accessible through the Context Menu action **History**.

### Differences Between Audit and History Sets

The Audit `[sys_audit]`, History Sets `[sys_history_set]`, and History `[sys_history_line]` tables store the same data, but they serve different purposes and manage data differently.

### Audit `[sys_audit]` table

The Audit `[sys_audit]` table is where the system stores historical information for all records. These records are intended to be kept forever so that administrators can always track the history of audited records. As the number of auditing records grows over time, it becomes more inefficient to directly query the Audit table for historical information. It is much more efficient to run queries only on the smaller subset records you actually want to view historical information for.
History Set [sys_history_set] table

The History Set [sys_history_set] table identifies which particular records from an audited table have historical information. The History [sys_history_line] table stores the actual changes to field values that occurred.

- The system automatically generates History Set and History records as needed from the Audit table when a user either creates a record or requests its history.
- Rather than containing a complete history of all changes in the system, History Set and History records only contain a recent subset of historical information for records where users have created or requested such information.
- In addition to audit data, history sets also include the information that is set during record insert, including journal field entries. Journal field entries you create before creating a record are handled in the same manner as journal entries created at the time of record creation. These journal entries appear in history sets with the same creation time and created by data as the associated record itself.

The system limits History Set and History records by:

- Having the table cleaner delete History Set records that have not been updated in 30 days.
- Using table rotation to rotate between four History tables every seven days. The system drops History records that are older than 28 days.

Should someone need historical information again at a later date, the system can regenerate it from auditing source records.

After the system generates History Set records, the context menu choice History uses the History Set rather than Audit records. From the user's perspective, the same historical data is available in the same user interface, but the way the information is stored is different.

Control access to history

You can give a role access to view audit history by setting a system property.

Role required: admin

1. Navigate to System Properties > System.
2. In the property List of roles (comma-separated) that can access the history of a record, enter the user roles you want to access history.
3. Click Save.

Any changes to a field are omitted if a user without read-access views the history of a record.

Change the number of history entries

By default, the history displays a maximum of 250 history entries, but you can change this value.

Role required: admin

1. Navigate to System Properties > System.
2. In the property Maximum number of field entries displayed in record history, default is 250, enter a new maximum number of entries.
History List

The history list displays each change as its own row in the change list.

<table>
<thead>
<tr>
<th>Label</th>
<th>Old</th>
<th>New</th>
<th>Type</th>
<th>Update number</th>
<th>Update time</th>
<th>User name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>global</td>
<td>TOP/ACME</td>
<td>Audit</td>
<td>3</td>
<td>2012-06-15 12:56:25</td>
<td>ITIL User</td>
</tr>
<tr>
<td>State</td>
<td>New</td>
<td>Active</td>
<td>Audit</td>
<td>3</td>
<td>2012-06-15 12:56:25</td>
<td>ITIL User</td>
</tr>
<tr>
<td>Incident state</td>
<td>New</td>
<td>Active</td>
<td>Audit</td>
<td>3</td>
<td>2012-06-15 12:56:25</td>
<td>ITIL User</td>
</tr>
<tr>
<td>Company</td>
<td>ACME</td>
<td></td>
<td>Audit</td>
<td>3</td>
<td>2012-06-15 12:56:25</td>
<td>ITIL User</td>
</tr>
<tr>
<td>Caller</td>
<td>Bud</td>
<td>Richman</td>
<td>Audit</td>
<td>3</td>
<td>2012-06-15 12:56:25</td>
<td>ITIL User</td>
</tr>
<tr>
<td>Assigned to</td>
<td>ITIL User</td>
<td></td>
<td>Audit</td>
<td>3</td>
<td>2012-06-15 12:56:25</td>
<td>ITIL User</td>
</tr>
<tr>
<td>Urgency</td>
<td>3 - Low</td>
<td></td>
<td></td>
<td>0</td>
<td>2012-04-05 17:42:29</td>
<td>System Administrator</td>
</tr>
</tbody>
</table>

View History List

Click on a row item to view additional details about the change.
View List Change

Requirements

To view a history list, the following requirements must be met.

- **Auditing**: Auditing for the table must be enabled to view a history list.
- **ACLs**: By default, the List history option is only available to users with the admin user role. To enable this option to non-admins, create a custom ACL rule granting read access to the Record History [sys_history_set] table.
- **Roles**: At least one of the roles that the user has must be included in the glide.history.role property, which includes the itil role by default.

History Calendar

The history calendar shows you the days where the record was changed, who made the change, and when.
The History Calendar is sorted by update number. Each user is assigned a color so you can tell at a glance how many
times a record was changed by a specific user. For example:

Changes made by system administrator

Changes made by ITIL user

To highlight changes to a particular field, select the field from the **Highlight changes to field** selection box.
Picking a field from this selection box changes the calendar to highlight the times that field was changed. Hover over
the text of one of a highlighted change to see the change in value.
If you hover over the icon within an entry, a popup displays all the value changes. This is the same information that is displayed in the top part of the form.
<table>
<thead>
<tr>
<th>Week</th>
<th>Mon</th>
<th>Tue</th>
<th>Wed</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>15</td>
<td>9</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>16</td>
<td>16</td>
<td>17</td>
<td>18</td>
</tr>
<tr>
<td>17</td>
<td>23</td>
<td>24</td>
<td>25</td>
</tr>
</tbody>
</table>

### Incident History Detail

**Details for INC0000039**

- **Created**: 2012-04-05 17:42:29 by admin
- **Last updated**: 2012-06-15 12:56:26 by itil
- **Update count**: 3 (1 audited)

- **Created by**: System Administrator (70 Days 1 Week)
- **Updated by**: ITIL User (2 Minutes)

**Field** | **Value**
---|---
Active | true
Approval | Not Yet Requested
Assignment group | Network
Caller | Bud Richman
Category | Network
Configuration item | MailServerUS

**Additional comments**: Routing from San Diego to the Oregon mail server appears to be getting packet lost!

- **Contact type**: Phone
- **Escalation**: Normal
- **Impact**: 3 - Low
- **Incident state**: New
- **Incident type**: Routing
- **Knowledge**: false
- **Location**: Salem OR
- **Made SLA**: false
- **Notify**: Do Not Notify
- **Number**: INC0000039
- **Opened**: 2012-04-05 17:41:01
- **Opened by**: Bud Richman
- **Priority**: 4 - Low
- **Severity**: 3 - Low
- **Short description**: Routing to oregon mail server
- **SLA due**: 2012-04-26 17:41:01
- **State**: New
- **Task type**: Incident
- **Domain**: global
- **Urgency**: 3 - Low
You can click on the day number to get a view of the changes for that day. You can also click on the week number to the left to get a the week view. You can scroll to and from month to month to see changes.

**History Timeline**

You can view a timeline of changes for a CI and for its related records, relationships, baselines, and proposed changes for the CI. Timelines are available for CIs in the Configuration Item [cmdb_ci] table or a descendant of this table, if auditing is enabled for the tables.

Role required: The ACL for this view is based on the roles defined in the `glide.history.role` system property, which by default is set to `itil`. Also, the user must have read access to the History Set [sys_history_set] table, which by default is granted to admin.

You can open a timeline when you view the history of a CI. You can specify the time period, time range, and properties that are displayed in the timeline. You can view either what has changed in a particular change set, or view the entire CI to better troubleshoot any issues. You can also display a timeline of changes to the CI's related records, and export and compare snapshots of the CI at any point in time.

CI changes are represented by bubbles in different shapes and colors along the timeline. The shape of each bubble represents a different type of change and the color of each bubble specifies whether the change is valid or invalid. CI baselines are represented by black circles that you can hover over to display more details. Click the ? icon to display bubble shape and color definitions, and point to a bubble to display details about the change set.

A change to a relationship is considered valid only if it was applied through change management. If the change was applied via the Proposed Changes framework, it is valid. For additional validation steps, see Create or edit a planned validation script.

---

**History Timeline view**

© 2021 ServiceNow, Inc. All rights reserved.
Timeline bubbles

**Note:** Proposed changes that do not have a planned start date are placed at future points of time.

**Timeline navigator**

Use the handles on both ends of the timeline navigator to extend or to shorten the time period that is shown.

You can scroll to a different period of time by clicking on the bottom part of the timeline navigator and then dragging the navigator to the left or right.

**Zoom**

By default, the timeline for the last month is shown. Next to the **Zoom** label above the timeline, you can select another time interval. You can select intervals from a minute to the entire period of data.

If there are many changes of the CI during the time period, the bubbles displayed might get too crowded. You can zoom in or out to spread the bubbles in either method:

- Change the time interval on the timeline. As you shorten the time interval, you zoom in, and as you lengthen the time interval, you zoom out.
- Select the section of the timeline that you want to zoom into.

**Property filter**

You can filter the bubbles that are displayed. By default, all bubbles are displayed, representing changes to all of the CI's properties. You can limit the view to display only the bubbles in which selected properties have changed and exclude bubbles in which only unselected properties changed.

The **Detail** and **Summary** views highlight properties within your filter scope that have changed. The changed properties are highlighted in light blue.

In the **Summary** view, you can choose to include all the properties of the CI, or only properties that have changed. If you choose to display all properties in the summary view, then changed properties are listed before unchanged properties.
Summary view

The **Summary** view displays snapshots of the CI's represented by each bubble. Each snapshot displays the changes to the CI's fields and relationships according to the change set. It displays old and new values before and after the change, and any relationships that were added or deleted.

Use the > and < buttons on both sides of the snapshot display to scroll through the next and previous change set records in a chronological order.

Detail view

The **Detail** view displays snapshots of the CI that correspond with the bubbles. Each snapshot includes the fields that are within the property filter scope, displaying the properties that have changed with a light blue background. Click on a bubble to display its corresponding snapshot of the CI. The data that is displayed is read-only.

Use the > and < buttons on both sides to scroll through the next and previous change set records in a chronological order.

**View timeline of changes to related records**

On the timeline of changes for a CI record, you can also view a timeline of changes for the CI's related records.

- Role required: admin
- Target table: the CI record must be in the Configuration Item [cmdb_ci] table or a descendant of this table.
- Auditing: must be enabled for the table containing the CI.

1. Open the timeline for the CI.
2. Click the **Related Records** icon and select related records from the **List of Related Records** to view. Click the Related Records icon again to display the related records timeline.

The timeline of changes to the CI's related records is displayed right above the CI's timeline. If you uncheck all related records, the related records timeline is hidden.

Hover over a change bubble on the related records timeline to display details about the change, such as date and number of changed properties. As you change the time interval in focus, or zoom in or out, it affects both the CI timeline and the related records timeline simultaneously.

**Export a snapshot of a CI**

You can export a snapshot of a CI from its timeline.

The CI must be in the Configuration Item [cmdb_ci] table or a descendant of this table. Auditing must be enabled for the table containing the CI.

Role required: admin

You can export a snapshot of the CI to an XML, PDF (Portal), or PDF (Landscape) format.

1. Open the timeline for the CI.
2. Select the bubble representing the time for which you want to export a snapshot of the CI.
3. Click the export icon ( ).
4. Select the file format to use for the export.
   You can download the file to your system for viewing.

**Compare CI snapshots**

You can compare the properties and relationships of a CI at two different points in its timeline.

The CI must be in the Configuration Item [cmdb_ci] table or a descendant of this table. Auditing must be enabled for the table containing the CI.
Role required: admin

1. Open the timeline for the CI.
2. Click Compare.
3. Select a Start date and an End date.
4. Click Compare.

Tracking changes to reference fields

Administrators can track changes to reference field display values.

Since reference fields only store an ID value, the system can normally only audit changes when the ID value changes. By default, the system does not audit changes when a reference field display value changes.

Consider the following situation. A user changes her name from Jane Smith to Jane Miller. Since the user name is the display value for the User table, any previous reference to Jane Smith instead refers to Jane Miller. If the administrator just updates the name of the existing user record, audit and history records will only display the new name Jane Miller. By default, the system does not provide a way to distinguish between changes made under the original user name versus those made with the new user name.

If your auditing policy requires tracking user name changes, you can:

- Create a new user record for the new name and deactivate the previous user record. The system preserves audit records for the old user name and creates future audit records with the new user name.
- Create custom fields and a business rule to save the previous name and the date of the name change. The system can use this information to construct the proper names in audit and history records.

Tracking inserts

By default, the system does not create Audit records for inserts because in a typical instance, inserts can account for over 80% of the size of the Audit table.

Not tracking inserts allows for better performance and a much smaller Audit table. Administrators can enable auditing of inserts by setting the `glide.sys.audit_inserts` property to `true`.

Tracking CI Relationships

Changes to a CI relationship (CI Relations, CI/User Relations, or CI/Group Relations) appear in the history of the items on both sides of the changed relationship regardless of whether the change was manual or a result of Discovery.

For example, if the computer alpha has a used by CI Relation with the computer beta, then the history for alpha has a record of when the relationship with beta was established, and likewise, the history for beta has a record of when the relationship with alpha was established. This example illustrates the history displayed when some CI Relations are established, and then one of the relations is removed:
CI Relationship History

The created bullet indicates the date that the CI, user, or group was created. The last activity bullet refers to when the relationships were last changed. If you don’t want to show CI relationship history for any or all CI relationship types, you can turn it off by disabling auditing on the CI relationship tables (CI Relationship [cmdb_rel_ci], CI/User Relationship Type [cmdb_rel_user_type], or Group Relationship [cmdb_rel_group]).

System logs

The System Logs module provides a variety of logs that you can use to troubleshoot and debug transactions and events that take place within the instance.

Access the following logs from the System Logs module:

<table>
<thead>
<tr>
<th>Log</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transactions</td>
<td>All application activity for an instance.</td>
</tr>
<tr>
<td>Email and Push</td>
<td>All email notifications and Push messages sent from all instances within the system.</td>
</tr>
<tr>
<td>Events</td>
<td>All system events that occur within the system.</td>
</tr>
<tr>
<td>Import</td>
<td>Data import activity within the platform.</td>
</tr>
<tr>
<td>Log</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Table Changes</td>
<td>Changes made to all tables in the system.</td>
</tr>
<tr>
<td>Outbound HTTP Requests</td>
<td>All outbound web services requests such as REST and SOAP requests.</td>
</tr>
<tr>
<td>Signature Images</td>
<td>Electronic signatures for the HR signature pad.</td>
</tr>
<tr>
<td>System</td>
<td>Warnings and errors for instance processes, records, and non-critical events, such as memory usage on the server machine.</td>
</tr>
</tbody>
</table>

Use the Log File Browser to search and download logs. You can also search archived logs in the log history.

**Other logs**

Your instance offers other logs in addition to those in the System Logs module. For example, the System Diagnostics module provides upgrade history and slow query logs, which you can use to gain insight into how queries are affecting platform performance. The Customer updates table records every change that is made in the system.

**System log**

View warnings and errors for instance processes, records, and non-critical events, such as memory usage on the server machine.

The following information is tracked in the system log:

- Workflows
- Configuration
- Chats sessions
- Transactions for each view of each page in the system, including load times for network, server, and browser
- Inbound and outbound email
- Events triggered in the system
- Imports and integrations
- System warnings, errors, and script logs
- Upgrade information for any plugin activations, update sets, or system upgrades

Log entries appear for the current day only. To view other log files, use the log file browser. This log provides the following information for all occurrences:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created</td>
<td>Date and time of the logging activity for the locale of the machine running the instance.</td>
</tr>
<tr>
<td>Level</td>
<td>Type of message. The levels are Debug, Error, Warning, and Information.</td>
</tr>
<tr>
<td></td>
<td>• A warning is an error that has been handled and recovered.</td>
</tr>
<tr>
<td></td>
<td>• An error is something that must be fixed.</td>
</tr>
<tr>
<td>Message</td>
<td>System-generated message regarding the nature of the occurrence.</td>
</tr>
</tbody>
</table>
Workflow logging

- Each activity executed, including:
  - Date and time started
  - Date and time ended
  - State, for example, Finished, Cancelled, Timed Out, Error
  - Result
  - Fault description, if there was an error
- Transition history, including:
  - Time of transition
  - Activity transitioned from
  - Activity transitioned to
  - Which transition was triggered
- Workflow log, including any log statements added to the workflow

Configuration information

- Action taken, including insert, update, and delete
- Category of change
- Comments recorded with the change
- Name of the change
- XML difference of the change
- Update set the change is associated to
- Date and time of the change
- User who made the change
- Table where the change was made
- Name of the object being changed
- Type of object being changed
- View the change was made in, for changes to forms or lists

Transaction logs

The transaction log records all browser activity for an instance. To aid in debugging of system issues, you can filter transaction logs by application scope, limiting transactions that appear to only those transactions originating in specific scopes.

The transaction log provides the following information for all activities.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created</td>
<td>Date and time of the application action for the locale of the machine running the instance.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Type</td>
<td>Type of recorded transaction.</td>
</tr>
<tr>
<td>Created by</td>
<td>User who created this activity.</td>
</tr>
<tr>
<td>Origin application</td>
<td>Application scope the transaction originated in. Global appears if the transaction originated in the global scope.</td>
</tr>
<tr>
<td>Response time</td>
<td>Round trip response time for the application request, in milliseconds.</td>
</tr>
<tr>
<td>Network time</td>
<td>Latency time of the network response after the application request is made, in milliseconds.</td>
</tr>
<tr>
<td>Output length</td>
<td>Size of the output string sent by the instance to the application, in bytes.</td>
</tr>
<tr>
<td>SQL count</td>
<td>Number of SQL server commands executed for this activity.</td>
</tr>
<tr>
<td>Business rule count</td>
<td>Number of business rules executed for this activity.</td>
</tr>
<tr>
<td>Business rule time</td>
<td>Elapsed time for the execution of the business rules for this activity.</td>
</tr>
<tr>
<td>URL</td>
<td>Application or module connected to by the client application.</td>
</tr>
<tr>
<td>System ID</td>
<td>System generated identifier of the client instance making the request. This ID is used for cluster environments in which several instances (nodes) communicate with the database.</td>
</tr>
<tr>
<td>IP address</td>
<td>IP address of the client making the request.</td>
</tr>
<tr>
<td>GZipped</td>
<td>Indication of whether a compressed Web page was requested by the application.</td>
</tr>
<tr>
<td>Protocol</td>
<td>HTTP protocol used by the application for this instance.</td>
</tr>
</tbody>
</table>

Client transaction timings

The Client Transaction Timings plugin enhances the system logs by providing additional information about the durations of transactions taking place between the client and the server.

You can track down performance issues to their source by viewing where the time is being consumed, and how time was spent during a transaction.

This plugin requires the Response Time Indicator to be enabled, and collects information from the following browsers:
- Firefox
- Internet Explorer
- Chrome

Client Transactions Information

Installing the plugin adds the **Client Transactions** module to the **System Logs** application. It provides a list of every logged transaction between client and server within the last day:
Client Transactions Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created</td>
<td>Moment the transaction was recorded.</td>
</tr>
<tr>
<td>Response Time</td>
<td>Number of ms spent by the server in fulfilling the transaction.</td>
</tr>
<tr>
<td>Business Rule Time</td>
<td>Number of ms spent by business rules triggered by the transaction.</td>
</tr>
<tr>
<td>SQL Time</td>
<td>Number of ms spent by the SQL database.</td>
</tr>
<tr>
<td>Client Response Time</td>
<td></td>
</tr>
<tr>
<td>(Load_completion_time) - (start_time). It is inclusive of server time.</td>
<td></td>
</tr>
<tr>
<td>Client Network Time</td>
<td>Number of ms spent by the network the client is connecting through.</td>
</tr>
<tr>
<td>Browser Time</td>
<td>Number of ms spent by the browser during the transaction.</td>
</tr>
<tr>
<td>Client Script Time</td>
<td>The number of ms spent executing client scripts.</td>
</tr>
<tr>
<td>UI Policy Time</td>
<td>Number of ms spent executing ui policy.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of transaction:</td>
</tr>
<tr>
<td></td>
<td>- Form</td>
</tr>
<tr>
<td></td>
<td>- List</td>
</tr>
<tr>
<td></td>
<td>- Other</td>
</tr>
<tr>
<td>Table</td>
<td>Name of table that appeared. For example, incident, change_request.</td>
</tr>
<tr>
<td>View</td>
<td>View for this form/list.</td>
</tr>
</tbody>
</table>

Client Detailed Information

A more detailed breakdown of the client timings for all Form rendering (but not list rendering) is also tracked. To see details, drill into a particular client transaction record and observe the related list at the base of the screen.

Client Detailed Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order</td>
<td>Order during the load in which this operation occurred.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of operation.</td>
</tr>
<tr>
<td>Name</td>
<td>Descriptive name of this particular operation</td>
</tr>
<tr>
<td>Duration</td>
<td>Number of ms this operation took to complete.</td>
</tr>
</tbody>
</table>
Push logs

Consult the push log to track the status of push notifications that are queued to send from your system.

To view the push log, navigate to System Logs > Push Notifications. Users are required to have the push_admin or admin role to view the push log.

Push log fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Claim</td>
<td>Identification number that is generated by the scheduled job that sends the push notification. This number is applied to the Claim field to ensure consistency across multiple push scheduled jobs.</td>
</tr>
<tr>
<td>Payload</td>
<td>Content of the push notification.</td>
</tr>
<tr>
<td>Queue count</td>
<td>Number of times that the system tried to send the push notification. The status of the push notification relates to its queue count.</td>
</tr>
<tr>
<td></td>
<td>• If the queue count is 0 for longer than expected, then there are no scheduled jobs that are trying to send the push notification.</td>
</tr>
<tr>
<td></td>
<td>• If the queue count is greater than 0 and the Type is success, then you can infer that this is how many times the system tried to send the push notification before finally sending.</td>
</tr>
<tr>
<td></td>
<td>• If the queue count reaches 10, the system stops trying to send the push notification. The Type changes to failure.</td>
</tr>
<tr>
<td>Request ID</td>
<td>Unique identification number for the push notification. Similar to the message ID for an email, the request ID is used as a correlation token for the push notification.</td>
</tr>
<tr>
<td>Type</td>
<td>Status to indicate whether the push notification has been sent. The Type column can have these values:</td>
</tr>
<tr>
<td></td>
<td>• failure: The message could not be sent.</td>
</tr>
<tr>
<td></td>
<td>• pending: The message is queued for processing.</td>
</tr>
<tr>
<td></td>
<td>• success: The message was successfully sent, although not necessarily received by the mobile device.</td>
</tr>
</tbody>
</table>

System email log and mailboxes

The system email log records all emails that the instance creates or receives. System mailboxes are filtered views of this log.

Every notification email that the instance creates or receives is recorded in an Email [sys_email] record. You can navigate to a log of these records at System Logs > Emails.

The System Mailboxes are filtered views of the Emails [sys_email] table. The instance assigns an email record to a system mailbox depending on the values of the Type and State fields. For more information, see System mailboxes.

The following fields can be included in the layout of the system log and any of the system mailboxes:
## Email log

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mailbox</td>
<td>The system mailbox that lists this email record. The instance sets the value of this field according to the values of the <strong>Type</strong> and <strong>State</strong> fields.</td>
</tr>
<tr>
<td>State</td>
<td>The current state of the email (Error, Ignored, Processed, or Ready).</td>
</tr>
<tr>
<td>Receive type</td>
<td>The type of inbound email (None, Forward, New, or Reply).</td>
</tr>
<tr>
<td>Type</td>
<td>The status of the email. Choices are:</td>
</tr>
<tr>
<td></td>
<td>• received: The server received this email.</td>
</tr>
<tr>
<td></td>
<td>• received - ignored: The server received this email, but it was ignored by the instance for inbound email action purposes. Typically, these emails are either spam or auto-replies. See the <strong>Error String</strong> field for details.</td>
</tr>
<tr>
<td></td>
<td>• send - failed: The server has attempted to send the email and failed. See the <strong>Error String</strong> field for details.</td>
</tr>
<tr>
<td></td>
<td>• send - ignored: The server skipped sending this email. Typically, this is for an email which was generated but lacked a recipient email address or is a duplicate email. See the <strong>Error String</strong> field for details.</td>
</tr>
<tr>
<td></td>
<td>• send - ready: The email is ready to be sent, but has not been sent out by the mail server. Typically, an email remains in this state for only a short time.</td>
</tr>
<tr>
<td></td>
<td>• sent: The email was sent by the instance without any errors or issues.</td>
</tr>
<tr>
<td>Target</td>
<td>A Document ID reference to the record if the email is generated by an insert, update, or delete of a particular record.</td>
</tr>
<tr>
<td>User</td>
<td>The name of the user, from the user record, of the instance from which the email notification was sent.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>This is a string field.</td>
</tr>
<tr>
<td>Notification Type</td>
<td>The type of notification. Choices are:</td>
</tr>
<tr>
<td></td>
<td>• None</td>
</tr>
<tr>
<td></td>
<td>• SMS</td>
</tr>
<tr>
<td></td>
<td>• SMTP</td>
</tr>
<tr>
<td>UID</td>
<td>The unique ID of the email stored on the server.</td>
</tr>
<tr>
<td>Created</td>
<td>The date and time of the email activity for the locale of the machine running the instance.</td>
</tr>
<tr>
<td>Deleted</td>
<td>For inbound email, indicates whether the email was deleted from the email server.</td>
</tr>
<tr>
<td>Weight</td>
<td>The weight of the email, which determines the sending priority relative to other notifications on the same table.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Importance</td>
<td>An indication that the email was sent with a changed level of importance, such as Urgent.</td>
</tr>
<tr>
<td>Originating Event and Notification</td>
<td>For emails generated by notifications, an embedded list that stores the event and notification that created the email.</td>
</tr>
<tr>
<td>Subject</td>
<td>The email subject. For notifications, you create the subject text in System Notification &gt; Email &gt; Notifications.</td>
</tr>
<tr>
<td>Error String</td>
<td>The error string captured from the email server to determine why the email was not sent. This is logged only if the email is send-failed.</td>
</tr>
<tr>
<td>Recipients</td>
<td>The email addresses of the recipients.</td>
</tr>
<tr>
<td>Body</td>
<td>The body of the email, displayed in raw HTML markup. Use the related link Preview HTML Body to see the body text as rendered HTML.</td>
</tr>
<tr>
<td>Content type</td>
<td>The email content type.</td>
</tr>
<tr>
<td>Headers</td>
<td>Any headers embedded in the email.</td>
</tr>
</tbody>
</table>

**Event logs**

The event log records all system events that occur within the Now Platform.

This log provides the following information for all events that occur:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created</td>
<td>Date and time of the event for the locale of the machine running the instance.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the event as listed in the Event Registry.</td>
</tr>
<tr>
<td>URI</td>
<td>HTTP query that generated the event.</td>
</tr>
<tr>
<td>Parm1</td>
<td>Event-specific value that depends on the event and the recipient.</td>
</tr>
<tr>
<td>Parm2</td>
<td>Event-specific value that depends on the event and the recipient.</td>
</tr>
<tr>
<td>Table</td>
<td>Database table acted on for this event.</td>
</tr>
<tr>
<td>Processed</td>
<td>Date and time the event was processed. This time reflects the locale of the machine running the instance.</td>
</tr>
<tr>
<td>Processing time</td>
<td>Time taken to process this event, in milliseconds.</td>
</tr>
<tr>
<td>Queue</td>
<td>Processor queue name.</td>
</tr>
</tbody>
</table>
Import logs

The import log displays information in a verbose format about any data import activity within the platform.

For a more detailed view of the import sets that produced a particular log, see Import Sets > Transform History.

This log provides the following information for all imports:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created</td>
<td>Date and time of the import for the locale of the machine running the instance.</td>
</tr>
<tr>
<td>Level</td>
<td>Type of message displayed. For import files, the level is Information.</td>
</tr>
<tr>
<td>Message</td>
<td>System-generated message regarding the status of the import.</td>
</tr>
<tr>
<td>Source</td>
<td>Name of the external source of the import, such as an integration.</td>
</tr>
</tbody>
</table>

System Diagnostics module

The System Diagnostics application provides logs that relate to the platform.

These logs are available:

- **Upgrade History**: tracks every upgrade to an instance.
- **Slow Queries**: provides insight into how queries affect platform performance. See Slow Query Logs.

Customer updates table

Every change that is made in the system is recorded on the Customer Updates [sys_update_xml] table chronologically.

To navigate to this table, enter `sys_update_xml.list` into the navigation filter. For information about update sets, see System update sets.

The following information is stored about each update:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name that identifies the updated record.</td>
</tr>
<tr>
<td>Created</td>
<td>The date and time the customer update record was created.</td>
</tr>
<tr>
<td>Created By</td>
<td>The user who performed the change.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of the update.</td>
</tr>
<tr>
<td>Updated</td>
<td>The date and time the customer update record was updated.</td>
</tr>
<tr>
<td>Updated By</td>
<td>The user who performed the update.</td>
</tr>
<tr>
<td>Updates</td>
<td>The number of times the record has been updated.</td>
</tr>
</tbody>
</table>
### Log history

The system uses table rotation and table extension to archive older logs.

By default, the system uses the following schedule to archive common logs:

#### Common log archive schedule

<table>
<thead>
<tr>
<th>Table</th>
<th>Archive schedule</th>
<th>Rotations</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event [ecc_event]</td>
<td>Every day</td>
<td>7</td>
<td>Rotation</td>
</tr>
<tr>
<td>Queue [ecc_queue]</td>
<td>Every day</td>
<td>7</td>
<td>Rotation</td>
</tr>
<tr>
<td>Event [sysevent]</td>
<td>Every day</td>
<td>7</td>
<td>Rotation</td>
</tr>
<tr>
<td>Log [syslog]</td>
<td>Every week</td>
<td>8</td>
<td>Rotation</td>
</tr>
<tr>
<td>Transaction Log [syslog_transaction]</td>
<td>Every week</td>
<td>8</td>
<td>Rotation</td>
</tr>
<tr>
<td>Email [sys_email]</td>
<td>Every 30 days</td>
<td>8</td>
<td>Extension</td>
</tr>
</tbody>
</table>

#### Use the log file browser

The instance provides the utilities log file browser and log file download.

Use **System Logs > Log File Browser** to view any system log entry. You can search for log files by using the following filters:

#### Log file browser

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start time</td>
<td>Start date and time of the range you want to search, for the locale of the machine running the instance.</td>
</tr>
<tr>
<td>Session ID</td>
<td>System-generated hexadecimal string that identifies the session that generated the log entry.</td>
</tr>
<tr>
<td>End time</td>
<td>End date and time of the range you want to search, for the locale of the machine running the instance.</td>
</tr>
<tr>
<td>Message</td>
<td>System-generated description of the occurrence.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>Level</td>
<td>Type of message displayed. The levels are Debug, Error, Warning, and Information. A warning is an error that has been handled and recovered. An error is something that must be fixed.</td>
</tr>
<tr>
<td>Thread name</td>
<td>System-generated identifier of the thread that created the log file.</td>
</tr>
<tr>
<td>Max rows</td>
<td>Maximum number of records returned for a particular filter.</td>
</tr>
</tbody>
</table>

The instance creates compressed archives of system logs every two days and purges log archives after 21 days. You can download log file archives and view them with System Logs > Log File Download. Select a log archive from the list, and then click Download log under Related Links to open or save the archive.

**Note:** Log files are only available for the node you are currently logged into. To see the currently logged into node, navigate to System Diagnostics > Stats.

**Antivirus Scanning**

Use Antivirus Scanning to help protect your instance against virus infections that can be introduced by file attachments to your system records, such as incidents, problems, and stories.

**Security scan**

Antivirus Scanning scans file attachments stored in your attachment [sys_attachment] table to help protect users from uploading and downloading infected files. All the document types supported by the Platform are scanned by Antivirus Scanning.

The Antivirus Protection plugin (com.glide.snap) is activated and enabled by default on your instance. As an administrator, you can deactivate and reactivate the Antivirus Scanning feature across your instance at the switch of a toggle, set configuration options, and review antivirus activity on the instance.

**Note:**
- Antivirus Scanning is also available for customers in the Government Community Cloud (GCC) and commercial environment. Users must set the (com.glide.snap.fed_enable_scan) property to True to start using the feature.
- Edge-encrypted files are excluded from this scan.
- Any file above 100 MB file size is not scanned.
- Inbound emails are scanned for viruses by system email filters, not by Antivirus Scanning.

**Scanning scenarios**

Review these upload and download scenarios to understand how the system identifies potential security threats from files attached to your records.

**Scenario 1 - Upload a file**

1. A user unknowingly uploads an infected file to a record.
2. The system scans the file and moves it to quarantine.
3. The file appears in the Attachments window, where it is marked as unavailable.
4. The user selects the file and this error message appears: The file Infected_testing.txt did not pass the security scan. Please remove the file from record INC0000059 and try again.
5. The system sends an email notification to the user and the antivirus administrator.
6. The user closes the Attachments window and is returned to the record, where the infected file displays as unavailable.

Scenario 2 - Download a file

1. A user opens a record to download a file that is attached to it.
2. Unaware that the file is infected, the user selects it for download.
3. The system scans the file, moves it to quarantine, and displays this message.

4. The user closes the message and the screen refreshes showing that the file is unavailable.
5. The system sends an email notification to the user and the antivirus administrator.

Scenario 3 - Download a ZIP file

1. A user opens a record and downloads a ZIP file that is attached to it.
2. The system scans the ZIP files individually.
3. One file does not pass the security scan and is marked as unavailable. The remaining files are zipped and downloaded successfully.
4. The user opens the ZIP file and sees an “error.txt” file in addition to the successfully downloaded file. This file contains an error message specifying which file did not pass scanning and was therefore not included in the ZIP.

5. The user opens the record again, and sees that the unavailable file has been moved into the Potential security risks section in the Attachments window and cannot be downloaded.

![Diagram of Attachments window with Potential security risks section highlighted.]

**Configure Antivirus Scanning**

Configure Antivirus Scanning across your instance and at the table level.

Role required: antivirus_admin or admin

Antivirus Scanning is active by default in your instance, where it automatically scans attachments to identify any files that are infected by viruses. You can also deactivate it in your instance if required. Configure the feature by ensuring the scan is enabled across your instance, and by identifying any tables that you want to exclude from the scan.

1. Navigate to Antivirus > Configuration.
2. As you configure the feature, consider the following.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Antivirus scanning</td>
<td>As antivirus scanning is active and enabled on your instance by default, its toggle is set to the on position and appears green in color. To disable the scanning across your instance, you can switch the toggle to the off position so it is no longer green.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Allow attachments to be downloaded when Antivirus scanner is unavailable</td>
<td>If this option is set to the on position, antivirus scanning is bypassed if the scanner times out and a response cannot be obtained. In this situation, the file download proceeds without completing the scan. If the option is set to off, the file download is prohibited until the scan can complete successfully.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>List of Tables Excluded</th>
<th>Any file attachments associated with a table in this list are excluded from antivirus scanning. Proceed to Step 4 if you want to define the tables the system excludes from scanning.</th>
</tr>
</thead>
</table>

3. Click **Save**.

4. Exclude tables from the Antivirus scan by adding them to the **List of Tables Excluded**.
   a) Navigate to **System Definition # Dictionary**
   b) Search for the table you want to exclude from the scan and select the table with Type set to collection.
   c) In the **Attributes** tab, click **New**.
   d) Add **Exclude_from_antivirus_scan** in the Attributes field and enter **True** in the **Value** field.
   e) Click **Submit**.

Antivirus Scanning is enabled in your instance, and the **List of Tables Excluded** on the Antivirus Configuration page is populated with all of the tables that you excluded from the scan.

**Dictionary attributes for Antivirus Scanning**

Dictionary attributes alter the behavior of the table or element that the dictionary record describes. As an administrator, you can set the values of dictionary attributes to modify the behavior of the default Antivirus Scanning configuration.

<table>
<thead>
<tr>
<th>Dictionary attributes for Antivirus Scanning</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Value</td>
</tr>
<tr>
<td>Exclude_from_antivirus_scan</td>
<td>true/false</td>
</tr>
<tr>
<td>Supress_antivirus_email_notification</td>
<td>true/false</td>
</tr>
<tr>
<td>Supress_antivirus_ui_notification</td>
<td>true/false</td>
</tr>
</tbody>
</table>

**Review quarantined files**

Review quarantined file attachments and take further action as needed.

Role required: antivirus_admin or admin
Monitor your quarantined file entries in the Antivirus Quarantine page at regular intervals to perform any of the following actions.

1. Navigate to **Antivirus > Quarantine**.
2. Select the **Actions on selected rows** check box next to each quarantined entry on which you want to perform any of these actions.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Delete</strong></td>
<td>Select this action to delete the quarantined file if it is not required any more by users.</td>
</tr>
<tr>
<td><strong>Restore</strong></td>
<td>Select this action to restore the file based on your assessment of its status or on the user request. However, scan the file with your third-party antivirus product before you restore it to mitigate any virus threats. Once restored, the file is available for download to the user.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Download</td>
<td>Select this action to download the file to your local system for further scanning and analysis, if desired.</td>
</tr>
</tbody>
</table>

The system asks for confirmation and performs the selected action per your input.

**Review antivirus activity**

Review the Antivirus Activities log that tracks all activities that occur on potentially-infected files from the point that they are discovered and placed into quarantine.

Role required: antivirus_admin or admin
This log functions as a report that captures antivirus activity, such as discovery, deletion, and other possible quarantined file events.

1. Navigate to **Antivirus > Activity**.
2. Review the log of quarantined files.

You can view the actions performed (highlighted in red) on each quarantined file.

Determine which records you want to delete, restore, download, or keep in the log. See **Review quarantined files**.
Virtual Private Network (VPN)

Use a virtual private network (VPN) to integrate your instance with external data sources over the Internet.

When configuring an integration that uses an encrypted protocol, such as Lightweight Directory Access Protocol (LDAP) or HTTPS, it is good practice to use the Internet as a transport mechanism.

However, there may be security or network architecture requirements that dictate the use of a site-to-site Internet Protocol Security (IPSEC) Virtual Private Network (VPN) connection between the datacenters and your business networks. The VPN supports the necessary encrypted communication between the instance and your network.

This video describes how to locate the IP addresses for each of your company's instances.

VPN connections

The ServiceNow VPN infrastructure uses pairs of Cisco adaptive security appliance (ASA) devices that serve as VPN termination points.

The VPN between the instance and your network utilizes your existing networking hardware to support communications. It is not necessary to install a piece of hardware. Because each customer has a unique configuration, the instance has a flexible VPN solution. The instance has built tunnels to Checkpoint, Juniper, Nortel, and other IPSEC VPN-capable devices.

The VPN connections between the instance and your network are created to support the encrypted flow of traffic into your network. Frequently, integrations that use the VPN do not have encryption as part of the underlying protocol. For example, LDAP over the VPN versus LDAPS over the Internet and HTTP over the VPN versus HTTPS over the Internet.

The network does not allow any inbound-to-ServiceNow integration or end-user-to-ServiceNow traffic to traverse a VPN connection. This restricted communication includes end-user access to the platform, administration of the platform, web services integrations, and other integrations that are configured to use a MID Server. All such inbound communication to the instance must be performed over the Internet using HTTPS. This configuration provides an encrypted communication channel. The encryption channel, along with IP access control, meets the security requirements for this traffic flow.

Addresses for VPN communication

To prevent conflict or overlap with internal ServiceNow networks or with another internal IP address schemes in your network, all tunneled traffic in the encryption domain must use non-RFC-1918 addresses on both sides of the tunnel.

ServiceNow provides a single IP address for the source of queries into your network. You must provide Network Address Translation (NAT), non-RFC-1918 addresses for each host that is integrating with your instance. These public addresses need to be owned by your organization. Third-party addresses cannot be used inside tunnels. Additionally, the encryption domain must not contain the IP address of the VPN peer.
Redundant tunnels

There are two ways to build redundancy for your tunnels:

- Using the same encryption domain behind both of your peers. This is the preferred method.
- Using a different encryption domain behind each peer.

With the first method, you need to provide the same NAT address behind each of your peers to create a connection path using that address to your server. The path to your server could be the same physical machine or a mirror which provides identical services. With this method, your instance would use the same IP address to connect to your servers regardless of whether your primary or secondary tunnel is active. If you have more than one server, follow this same scheme for your additional servers. This method provides the most transparency to your users and is recommended.

The second method requires configuration in your instance to provide the redundancy. When the tunnel is used for LDAP, for example, you could provide redundant LDAP servers in your instance. Note that this method requires the connection to the first configured LDAP server to timeout before the instance attempts to connect to the secondary server. Because of this additional time delay, this solution should only be implemented if the first option is unattainable. Also note that not all services can be configured for redundantly in your instance. If you are using a VPN tunnel for something other than LDAP and redundancy is required, check that your configuration can support multiple addresses, or see the first option above.

Alternatives to using a VPN

These alternatives provide a simpler way to connect your instance to the resources in the ServiceNow data centers and provide better encryption. Additionally, you can avoid any issues that VPN downtime might cause, such as making your instance unavailable to users if there is an issue with the VPN tunnel.

Single sign-on and MID server

Consider using a combination of Single Sign-On (SSO) for authentication and the MID Server for user data synchronization, rather than using a VPN to connect your LDAP server to your instance. For integrations other than LDAP, consider using certificate-based encryption.

You can use the LDAP listener on a MID server to synchronize your user table in near real time. The advantage of this approach is that there are no firewall holes, routes, VPN tunnels, or other special network settings to configure and maintain. The SSO/MID-Server solution is the most flexible, secure, and cost-effective method to achieve the complete LDAP integration.

LDAP over SSL

Another alternative to using a VPN tunnel is to configure LDAP Over SSL (LDAPS) directly over the Internet. You can configure a read-only domain controller and lock the instance down in your DMZ using only the instance's source addresses and the destination ports of your choice. Since the ports for LDAP are configurable in your instance, you can perform a port address translation (PAT) if desired. With LDAPS, you control the certificate that is uploaded over an encrypted channel to the instance, (see Upload a certificate to an instance). The packets cannot be encrypted or decrypted without the certificate.

The advantage of this approach is that it provides a stronger encryption and decryption mechanism. A VPN can only encrypt and decrypt the traffic between the two peers sitting on the Internet with a coordinated pre-shared key, similar to a password. LDAPS provides a longer encrypted path, end-to-end, at the application layer and with a certificate that is far more complicated than a pre-shared key that the IPSec tunnel uses.
VPN setup

From the time that a VPN request is submitted, it typically takes one week or less to complete the VPN build. To support the redundancy requirements of your instance and your organization, a minimum of two and a maximum of four VPNs are provisioned (from the active site to your active site or the active site to your DR site, and so on).

It is good practice for the encryption domain to be as specific as possible. Ideally, the encryption domain would include only the specific hosts that are required for the integrations. A large encryption domain can create opportunities for routing discrepancies (VPN versus Internet).

To create the VPN, the instance does the following:

1. Provides the VPN peer and host addresses from each data center.
2. Builds the necessary VPN connectivity from two data centers into your network. To support redundancy and disaster recovery (DR) requirements, the VPNs can be provisioned from two data centers into two networks.

The instance does not support building multiple VPN tunnels into a customer network for the purpose of connecting to multiple geographic regions or subsidiaries. You should perform any inter-site routing, traffic distribution, or traffic shaping within your own internal network, rather than having multiple VPN tunnels.

Request a VPN service

For all VPN requests, including provisioning, modifications, or general questions, use the Service Catalog VPN Request form.

1. Open HI.
2. Navigate to Self-Service > Service Requests > VPN Requests.
3. Select the appropriate VPN request type.
4. Answer the questions. Questions vary depending on the request type selected.
5. Click Submit.

Once your request is submitted, ServiceNow will work with your network engineer(s) to test and validate that the VPN is successfully passing traffic. To ensure that your questions are answered in a timely manner, please address VPN-related questions during this process.

Create an address for VPN communication

To prevent conflict or overlap with internal ServiceNow networks or with another customer's internal IP address schemes, the instance requires that all tunneled traffic in the encryption domain use non-RFC-1918 addresses on both sides of the tunnel.

The instance provides a single IP address for the source of queries into your network.

- Provide Network Address Translation (NAT), non-RFC-1918 addresses for each host that is integrating with the instance.

Domain separation for service providers

With the ServiceNow Platform, service providers (SPs) can provide their customers with faster onboarding, meet compliance, and protect their data using domain separation. Separate client data, processes, and reports into logical groupings called domains. SPs control who sees and accesses what content.

Watch this short video for an overview of domain separation.
## Explore, learn, develop

<table>
<thead>
<tr>
<th>What's new in Quebec</th>
<th>See the latest offerings in this release.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recommended practices</td>
<td>Tips and tricks for creating your domain structure wisely</td>
</tr>
<tr>
<td>Concepts for service providers</td>
<td>Concepts that work with the ServiceNow platform to help you solve for common use cases</td>
</tr>
<tr>
<td>Support levels by application</td>
<td>Is your favorite application supported for domain separation? Discover application support levels and use cases.</td>
</tr>
<tr>
<td>Safe Workplace Suite and domain separation</td>
<td>ServiceNow Safe Workplace applications help you reopen your workplaces and support the health and safety of your employees after emergencies and pandemics like COVID-19. The suite has many applications, including those for Emergency response, to help your organization mobilize, recover, and rebuild. All Safe Workplace applications support domain separation.</td>
</tr>
<tr>
<td>Classes</td>
<td></td>
</tr>
<tr>
<td>• For developers: ServiceNow Developer Site Domain Separation</td>
<td></td>
</tr>
<tr>
<td>• For service providers: Domain Separation for Service Providers (Now Learning login required)</td>
<td></td>
</tr>
<tr>
<td>Setup and administration</td>
<td></td>
</tr>
<tr>
<td>• Upgrade to Quebec</td>
<td></td>
</tr>
<tr>
<td>• Request domain separation</td>
<td></td>
</tr>
<tr>
<td>• Create a domain</td>
<td></td>
</tr>
<tr>
<td>Troubleshoot</td>
<td></td>
</tr>
<tr>
<td>• Search the Known Error Portal for known error articles</td>
<td></td>
</tr>
<tr>
<td>• Contact Customer Service and Support</td>
<td></td>
</tr>
<tr>
<td>• Ask or answer questions in the community</td>
<td></td>
</tr>
</tbody>
</table>
What's new in Quebec for service providers

See what's new in the Quebec release with domain separation for service providers.

New in Quebec

Domain Separated Tables
See at a glance which tables are domain-separated in your instance.

Domain Override Viewer
See and manage all your process overrides at once across the entire instance.

IntegrationHub Remote Process Sync
When integrations require the transform and mapping of data across different tables between two instances, ServiceNow remote system administrators can now use generic record management actions to integrate any two tables. See also the IntegrationHub Release Notes.

Subscription Management Domain Specific Reporting
System administrators with a new dashboard can enable program and account management with greater detail on license and subscription unit consumption, making cost recovery easier.

ITOM: Global MID-Server for Cloud Provisioning and Governance (CPG)
Service providers can provision a single MID-server to handle certain cloud actions in CPG without having to managing multiple, discrete MID-servers. See also the ITOM Optimization release notes.

Platform User Interface (UI) Builder
With the UI Builder with domain separation, support system administrators and delegated developers can build modern user interfaces and actions in a visual design studio without costly customizations. See also the UI Builder release notes.

Quebec release notes
ServiceNow domain separation product enhancements and updates in the Quebec release

Understanding domain separation
With domain separation you can separate data, processes, and administrative tasks into logically defined domains.

Domain separation is best for those customers who:

- Need to enforce absolute data segregation between business entities (data separation).
- Customize business process definitions and user interfaces for each domain (delegated administration).
- Maintain some global processes and global reporting in a single instance.
- Separate data between service providers, customers, partners, or sub-organizations.
- Have minor or moderate process differences among customers.
Domain separation compared to separate instances

While domain separation provides multi-tenancy support, multi-tenancy is still contained within a single instance. Some global properties, data, and processes are shared across all domains. For example, having the system Remember me on the login page of the system is global and cannot be specified per domain.

If you need complete and total separation of all system properties and do not require global reporting or global processes, then separate instances are the best option.

Data separation

Members of a domain see only the data contained within their domain or the child domains that are lower in the domain hierarchy. By default, all users and all records are members of the global domain unless an administrator assigns them to a particular domain. Once you assign a user or a record to a domain, the instance compares the user's domain to the record's domain to determine whether the user can view the record.

ServiceNow applications are defined with the following incremental support levels. These levels are based on the perspective of actual use cases and personas.

**Data Separation:** Tenants see only data that they have permissions to see. Tenants can be granted access to other tenant data, but cannot query tenant data if they don't have access.

**UI Separation:** Supports a tenant-specific experience for UI elements such as views, lists, labels, and so on.

**Business Logic Separation:** You can create tenant-specific system policies such as email notifications, business rules, client scripts, UI policy, and UI actions.

**Hierarchical Modeling:** Nested-multi-tenancy so parent tenants can access child tenant resources. Business logic for parent tenants runs automatically for child tenants, and can be overridden at any level.

**Cross-Tenant Intelligence (Domain Scope):** Handles automatically the data, metadata, business logic, and processing context for tenants that have access to additional tenant data.

In general, data defined at a higher level in the domain hierarchy is not visible at lower levels in the hierarchy.
Domain path migration

Domain paths are used for all customers. Domain numbering is not used. Customer Service and Support can assist in the upgrade.

Alternatives to domain separation

Separate instances are a common alternative to domain separation. This provides a great degree of flexibility in meeting the requirements for customers and stakeholders with little to no impact on others.
Warning: Before activating domain separation, consult your representative to verify that it is suitable for your environment. Domain separation adds a level of administration overhead. Although it can be disabled, it cannot be removed from an instance.

Domain assignment

By default, domain separation adds a domain field to tables and their extensions.

You can also extend domain separation to any new tables you create by adding a `sys_domain` field to the table's dictionary definition. By default, the system only domain-separates platform and baseline application tables where appropriate.

Warning: ServiceNow does not recommend domain-separating platform tables (any table with the `sys_` prefix such as the Dictionary Entry [sys_dictionary] and Dictionary Entry Override [sys_dictionary_override] tables) because it can produce unexpected results.

Each record is assigned a single domain. That domain is stored in the `sys_domain` field. Several tables, by default, have the `sys_domain` column and are already domain separated.

The value of the `sys_domain` field contains the domain assigned to the record by any of the following:

- Company to which the user belongs
• Business rule when creating record
• Module used when creating record
• Form template used when creating record
• Domain of the parent record
• Domain assigned to User record
• Domain of the user who creates it

The system prevents the following tables from being domain separated:

• Access Control [sys_security_acl]
• Script Include [sys_script_include]
• System Property [sys_properties]
• Security Exclusion/Inclusion List Entities [sys_security_restricted_list]
• Dictionary Entry [sys_dictionary]
• Dictionary Entry Override [sys_dictionary_override]

Assigning users to companies

Administrators can quickly assign users to a domain by assigning them to a company. After users are assigned to a domain, records automatically inherit the user's domain.

For example, assigning Bow Ruggeri to the ACME company automatically assigns him to the ACME domain. Assigning Don Goodliffe to the Initech company automatically assigns him to the Initech domain. Any records they create are automatically added to the appropriate domain.

Adding a user to a domain by setting the company

Using business rules to assign domains

Administrators can use a business rule to automatically set a domain value when creating a record. The business rule must set a value in the sys_domain field. Administrators must ensure there is a sys_domain column available for the record’s table. To learn more see Domain separation recommended practices for service providers.
Using modules to assign domains

Administrators can use the **sysparm_domain** URL parameter to automatically assign new records to a particular domain from a module. Administrators must create a module with an **Argument** value of: `sysparm_domain=sys_ID of domain`.

Using form templates to assign domains

Administrators can use a form template to automatically assign new records to a particular domain. Administrators must add the **sys_domain** field to the form and select a domain value. For example, setting the **sys_domain** field to **TOP/ACME domain** automatically assigns all records from this template to the TOP/ACME domain.

Domain inheritance on tables

By default, related records inherit the domain of the parent record. For example:

- A change task record inherits the domain of the parent change request record.
- A problem record inherits the domain of the parent incident record.

Automatic domain assignment based on user domains

If no other domain conditions apply, a record automatically inherits the domain of the user who creates it.

Visibility domains and Contains domains

Visibility domains control what a specific user can see, while "contains" domains control what an entire domain of users can see.

Visibility domains

The "Visibility domains" element is in a related list on the user record that determines whether users from one domain can access records from another domain. Granting users a visibility domain grants all the rights they would normally have to the record based on ACL (access control list) rule permissions.

A visibility domain:

- Is a user-to-domain relationship and is explicitly granted.
- Is not a child domain.
- Is not controlled by the selection in the domain picker. Once users are granted access to a visibility domain, they always see data in that domain and its child domains.

> **Note:** Using visibility domains excessively is not recommended. Although visibility is one method to allow users to access records, it's best to use contains domains for more robust control.

Contains domains

Normally parent-child relationships define the domain hierarchy. A contains domain lets you relate domains on an as-needed basis, independent of parent-child relationships. However, contains domains grant visibility only to domain data. Processes remain unaffected by contains relationships.
A contains domain:

- Is a many-to-many, domain-to-domain relationship.
- May have child domains. When a domain is selected, you can see the data from that domain and its children.
- Is controlled by the selection in the domain picker.

**Note:** When you open the domain record, the scope is set to that record's domain, so you can see only child domains. Choose **Toggle Domain Scope** from the menu to populate the related list.

Contains domain example

When a user's home domain is A, and the A domain contains domains B and C, they all become peer domains. That means the user sees data from domains A, B, and C while in their home domain A. If users change domains with the domain picker to Domain B, they see only data in Domain B. When users interact with a record from Domain B or Domain C directly, they see only data for that domain.

Visibility domain example

Using domain visibility, if Don Goodliffe is in the Database domain, and Bow Ruggeri is in the Network domain, and no incidents are in the global domain, then Don cannot access Bow’s incidents because of data separation.
Inheriting visibility domains based on group membership

If you set the domain table to the Group [sys_user_group] table, users can inherit visibility domains based on their group membership.

Domain scope

Domain scope defines what users can and cannot access.

Every user has two domain scopes when establishing a session in a domain-separated instance.

- **Session scope** is set upon session establishment to the domain listed in the user's user record. Users can manually change their session domain scope from the domain picker.
- **Record scope** uses the domain of the record and is active when viewing the form of any record.

By default, the record scope takes precedence over the session scope so that users in higher level domains adhere to each record's data and process constraints. However, these users can choose to expand or collapse the domain scope to show or hide data from other domains. For example, a user in the Service Provider (SP) domain also has visibility into child domains such as the ACME domain. When looking at an incident record from the ACME domain, the user can choose to expand the domain scope to show values from the SP domain or collapse the domain scope to show only record values that match the record's ACME domain.

**Note:** Users always have access to data from domains that have been explicitly granted to them by domain visibility.

Users with the domain_expand_scope user role can select the domain scope from the **Toggle Domain Scope** UI action on the form. When record scope is in effect, click the UI action to expand to session scope and display all data available based to the user's domain and child domains. When session scope is in effect, click the UI action to collapse to record scope and display only data that matches the current record's domain.

**Note:** A record does not display the UI action to toggle the domain scope if the record is in the global domain or if the user's domain matches the record's domain.

Record value selection from other domains

Users who can see multiple domains have the option to select record values from a domain that is different than the record's domain.

For example, service desk agents working for a service provider might want to assign certain incidents to themselves to resolve issues on behalf of their customers. When they do this, the incident **Assigned to** field might contain a user from the SP domain, even though the incident record itself is associated with a child domain such as ACME.

Selecting a record value from another domain does not change the record's domain. The record retains its original domain. When a user views a record with values from multiple domains, the user's domain visibility determines what they see.
Record value selection

<table>
<thead>
<tr>
<th>When these conditions are met</th>
<th>The user has access to these UI elements</th>
</tr>
</thead>
</table>
| The user has access to the domain of the current record referenced in a field. | The user can:  
  - See reference field display value. For example, sees the user name in the **Assigned to** field.  
  - See the related record from reference icon. For example, sees the user record for the user in the **Assigned to** field.  
  - Select values from any visible domain. For example, can select users from either the SP and ACME domains. |
| The user does not have access to the domain of the current record referenced in a field. | The user can:  
  - Not see reference field display values. (This is the case if domain separation was activated in Madrid or later releases and the user doesn't have access to the domain of that record.)  
  - Only select values from the record's domain. For example, can only select users from the ACME domain. |

Domains and associated companies

With domain separation you can cascade changes you make to a company record to the domain and other records associated to the company.

By default, the system automatically assigns users to the same domain as their company. For example, all users of the ACME company automatically become members of the TOP/ACME domain.

**Note:** Users with the admin role can change their own user records and therefore change domains. Service Providers may want to either disable delegated administration or set up an approval process to verify that the user needs the admin role.

When you change a company's domain, the instance automatically changes the domain of the following associated records to match the company's new domain.

- Locations
- Departments
- Groups
- Users

**Note:** The instance does not automatically change the domain of any record where you have selected the Managed domain checkbox.

Domain deactivation and associated companies

When you deactivate a domain, the instance also automatically completes the following actions.

- Deactivates all companies in the domain.
• Prevents all users assigned to the inactive company from logging in.

**Note:** When a user from an inactive company attempts to log in, the user sees an error message.

For example, if you deactivate the ACME domain from the sample data, the instance also deactivates the ACME company, and the three sample users are locked out.

![Login error message example](image)

**Concepts for service providers**

These concepts work with the existing ServiceNow platform capabilities to help you solve for common use cases.

**Global queue**

The global queue concept provides a single virtual view of tasks that reside in multiple instances. The concept creates a custom application using remote tables to provide a fulfiller view of work that resides in multiple instances without having to replicate tasks or data. The concept can also be used to create a single view of an employee's requests in multi-instance environments.
Overview

Service Providers with agents working on tasks from multiple systems tend to integrate the data back to a central instance, or a “swivel chair” between instances. While this method might be appropriate in some cases, it can be expensive and time-consuming to build and maintain. This method also opens the provider up to potential auditing and data requirement considerations such as General Data Protection Regulation (GDPR) in all of the instances where the data now lives.

Global queue is an alternative: With this method, agents can see data assigned to them from a single instance without sovereign data persisting on the instance they are logged into. For example, in cases where clients have data residency requirements, but allow access by agents from other countries, the provider could use a “follow-the-sun” Help Desk using global queue.

Learn more about the Global Queue v.2 Proof of Concept on the ServiceNow Knowledge site.

Note: In the Quebec release forward, the Global Queue Proof of Concept has been upgraded to Global Queue v. 2.

Service provider connector
The service provider connector application is a reference design for creating a ServiceNow Store application for your customers to use to integrate with your systems. Service provider applications help you speed on-boarding and create standardized integrations.
Benefits of service connectors

When service providers (vendors, suppliers, partners) publish connectors, customer on-boarding is faster, which means faster billing. Integrated instances increase productivity, greater visibility in the ServiceNow ecosystem, and partner program benefits. Specific benefits are:

- Eliminates custom integrations, including the cost of services required to deliver and maintain them.
- Services are provider-defined within their ServiceNow instances and remove the need for the complexity and cost of custom integrations.
- Workflows and catalog requests can be synchronized, with the customer’s processes and approvals preceding the provider’s processes, so customers can follow their own processes.
- Any data created or modified (e.g. CIs) for the customer on the provider’s instance can be synchronized back into the customer’s instance for their visibility and use in processes.

Key features

User Interface

A service connector should include the following UI components at a minimum:

- Reports/Dashboards – Reports and dashboards pre-defined by persona help with visibility.
- Menu and modules – The customer should be able to find the application via descriptive Menu **Provider XYZ Services**.
- Roles – Every connector requires user and admin roles to ensure access can be controlled by the customer. For example, “x_snc_xyz_user” or “x_snc_xyz_admin”.
- On-boarding – Rapid on-boarding is essential to a good customer experience and should be included via playbook, guided setup, or catalog item in such a way that no professional services are required for the customer to go live. (Professional services are available, but on-boarding can be achieved without it).
- Configuration – Data points should be built into processes to account for most of the normal process configuration a customer needs to achieve. This eliminates professional services as much as possible.
- Documentation – Thorough documentation increases customer satisfaction and ease of use.
- Support integration or contact info – The customer needs an easy way to stay in contact with the service provider for any issues, questions, or requests.

Tasks

- The **eBonding** of tasks such as incidents, case, changes, problems, and so on, should be predefined in the connector. These integrations are built using Flow Designer and IntegrationHub to ensure the highest level of resiliency and performance.
CMDB

- Core data synchronize such as the CIs required for proper ITIL processes should be kept in sync between provider and customer instances.

Workflows

- All workflows should be designed in Flow Designer to ensure resiliency and performance.

Catalogs

- The provider’s catalog that the customer requests from should be included in the application as a record-producing catalog. The request generated by the item in the customer’s instance should be eBonded with the provider’s instances. The provider’s workflows keep the request updated and synchronize back to the customer’s instance.

Customer Processes

- Any mechanisms for syncing requests with the provider’s instance should allow for customer processes to interact with the requests before they are sent to the provider’s instance. During provider processing, approvals can be sent to the customer’s instance as needed.

Integration

- Integrations should be built using Flow Designer and IntegrationHub to ensure the highest level of resiliency and performance.

Possible components you can include in a Service Connector

Instance data replication (IDR): when replication is the goal

- Can be used for process integration, but can be too rigid depending on the complexity integration logic based on state transition
- To learn more, see Instance Data Replication

IntegrationHub: When process integration is the goal

- Easier to inject in the middle of a process, as part of complex or conditional step in the middle of a flow
- To learn more, see IntegrationHub

Global Work Queue (Virtual): when task federation is the goal, and storing data externally is not acceptable

- Used where agents are working across multiple ServiceNow instances and need to see all open work assigned to them
- Rows returned should be limited to less than 1000
- To learn more, see Global work queue

Remote Tables: when external data usage without storage is the goal

- Used to connect an instance to third-party sources, or to another instance, to retrieve external data and optionally cache it in the memory. The data is treated as a table in the instance for read-only purposes such as group, sort, aggregate, and filter.
- To learn more, see Retrieving external data using remote tables and scripts

Flow Designer: when process design is the goal

- Used for automating processes in a single design environment. Process owners can use natural language to automate approvals, tasks, notifications, and record operations without coding.
• To learn more, see Flow Designer

Learn more about the Service Connector proof of concept on the ServiceNow Knowledge site.

Installed with domain separation

Several platform components are added or modified with domain separation.

Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
</table>
| domain_admin     | Can create, edit, and delete domains.

Additions to [sys_domain] fields

The sys_domain field is added to the following tables:

Tables with the sys_domain field

<table>
<thead>
<tr>
<th>Tables</th>
</tr>
</thead>
<tbody>
<tr>
<td>sys_attachment</td>
</tr>
<tr>
<td>sys_user_has_role</td>
</tr>
<tr>
<td>sys_group_has_role</td>
</tr>
<tr>
<td>sys_email</td>
</tr>
<tr>
<td>sys_user_group</td>
</tr>
<tr>
<td>core_company</td>
</tr>
<tr>
<td>cmn_location</td>
</tr>
<tr>
<td>cmn_department</td>
</tr>
<tr>
<td>sys_gauge</td>
</tr>
<tr>
<td>sys_report</td>
</tr>
<tr>
<td>kb_feedback</td>
</tr>
<tr>
<td>sysapproval_approver</td>
</tr>
<tr>
<td>sys_user_grmember</td>
</tr>
</tbody>
</table>

Field for the Task Table

MSP Extensions add a task_for field to the Task table. This reference field refers to the User table.
The task_for column on the Task table

Options for the Group Type

MSP Extensions add several new default options to the type field of the Group table. Add to or update these types as needed to support your domains.

<table>
<thead>
<tr>
<th>Tables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td></td>
</tr>
<tr>
<td>Support</td>
<td></td>
</tr>
<tr>
<td>Visibility</td>
<td></td>
</tr>
</tbody>
</table>

Business rules

<table>
<thead>
<tr>
<th>Name</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain - Activate/Deactivate</td>
<td>core_company</td>
<td>Activates the related domain if at least one of its companies is active. Deactivates the related domain if all related companies are inactive.</td>
</tr>
<tr>
<td>Domain - Cascade Company</td>
<td>core_company</td>
<td>Keeps a company's domain in sync with its users, groups, departments, and locations.</td>
</tr>
<tr>
<td>Domain - Cascade Domain - Email</td>
<td>sys_email</td>
<td>Keeps an email's domain in sync with its attachments.</td>
</tr>
<tr>
<td>Domain - Cascade Domain - Group</td>
<td>sys_user_group</td>
<td>Keeps a group's domain in sync with its inherited roles (sys_group_has_role records).</td>
</tr>
<tr>
<td>Domain - Cascade Domain - Knowledge</td>
<td>kb_knowledge</td>
<td>keeps a knowledge article's domain in sync with its related feedback.</td>
</tr>
<tr>
<td>Name</td>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Domain - Cascade Domain - Task</td>
<td>task</td>
<td>Keeps the domain in sync with related tasks for wf_context, wf_executing, wf_history, attachments, emails, task_sla and its workflow, sysapproval_approver and its workflow, and sysapproval_group and its workflow.</td>
</tr>
<tr>
<td>Domain - Cascade Domain - User</td>
<td>sys_user</td>
<td>Keeps a user's domain in sync with its group membership (sys_user_grmember) and role (sys_user_has_role) records.</td>
</tr>
<tr>
<td>Domain - Cascade Domain - Version</td>
<td>wf_workflow_version</td>
<td>Keeps domains in sync with related workflow versions for wf_activity and wf_transition.</td>
</tr>
<tr>
<td>Domain - Deactivate Companies</td>
<td>domain</td>
<td>Deactivates related companies if a domain is deactivated.</td>
</tr>
<tr>
<td>Domain - Default - Task</td>
<td>task</td>
<td>Sets the task domain based on the Task for user's domain. If this domain would be global, sets domain to Default instead.</td>
</tr>
<tr>
<td>Domain - Default - User</td>
<td>sys_user</td>
<td>Sets a user's domain to Default if the domain otherwise would have been global.</td>
</tr>
<tr>
<td>Domain - Disallow Global Domain Record</td>
<td>domain</td>
<td>Prevents creation of a domain with the name global.</td>
</tr>
<tr>
<td>Domain - Override Copy</td>
<td>sys_app_application</td>
<td>When an application is overridden for a domain, creates a copy of its modules for the new application.</td>
</tr>
<tr>
<td>Domain - Override Copy</td>
<td>sys_data_policy2</td>
<td>When a data policy is overridden for a domain, creates a copy of its data policy rules for the new data policy.</td>
</tr>
<tr>
<td>Domain - Override Copy</td>
<td>sys_gauge</td>
<td>When a gauge is overridden for a domain, creates a copy of its gauge counts for the new gauge.</td>
</tr>
<tr>
<td>Domain - Override Copy</td>
<td>sys_ui_action</td>
<td>When a UI action is overridden for a domain, creates a copy of its UI action views for the new UI action.</td>
</tr>
<tr>
<td>Domain - Override Copy</td>
<td>sys_ui_list_control_embedded</td>
<td>When an embedded list control is overridden for a domain, creates a copy of its client and server scripts for the new embedded list control.</td>
</tr>
<tr>
<td>Domain - Override Copy</td>
<td>sys_ui_policy</td>
<td>When a UI policy is overridden for a domain, creates a copy of its UI policy actions for the new UI policy.</td>
</tr>
<tr>
<td>Domain - Set Domain - Approvals</td>
<td>sysapproval_approver</td>
<td>Sets the domain based on that of the record being approved.</td>
</tr>
<tr>
<td>Name</td>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Domain - Set Domain - Attachment</td>
<td>sys_attachment</td>
<td>Sets the domain based on the parent record's domain.</td>
</tr>
<tr>
<td>Domain - Set Domain - CMDB_CI</td>
<td>cmdb_ci</td>
<td>Sets a CI's domain to that of its company.</td>
</tr>
<tr>
<td>Domain - Set Domain - Department</td>
<td>cmn_department</td>
<td>Sets a department's domain to that of its company.</td>
</tr>
<tr>
<td>Domain - Set Domain - Domain</td>
<td>domain</td>
<td>Sets a domain's domain to itself.</td>
</tr>
<tr>
<td>Domain - Set Domain - Email</td>
<td>sys_email</td>
<td>Sets the domain based on the parent record's domain. An email's parent record is the record specified in the instance field.</td>
</tr>
<tr>
<td>Domain - Set Domain - Feedback</td>
<td>kb_feedback</td>
<td>Sets a knowledge feedback's domain to that of its knowledge article.</td>
</tr>
<tr>
<td>Domain - Set Domain - Group</td>
<td>sys_user_group</td>
<td>Sets a group's domain to that of its company.</td>
</tr>
<tr>
<td>Domain - Set Domain - Group Approvals</td>
<td>sysapproval_group</td>
<td>Sets the domain based on that of the record being approved.</td>
</tr>
<tr>
<td>Domain - Set Domain - Group Role</td>
<td>sys_group_has_role</td>
<td>Sets a group role's domain to that of its group.</td>
</tr>
<tr>
<td>Domain - Set Domain - Location</td>
<td>cmn_location</td>
<td>Sets a location's domain to that of its company.</td>
</tr>
<tr>
<td>Domain - Set Domain - Task SLA</td>
<td>task_sla</td>
<td>Sets a task SLA's domain to that of its task.</td>
</tr>
<tr>
<td>Domain - Set Domain - User</td>
<td>sys_user</td>
<td>Sets a user's domain to that of its company.</td>
</tr>
<tr>
<td>Domain - Set Domain - User Role</td>
<td>sys_user_has_role</td>
<td>Sets a user role's domain to that of its user.</td>
</tr>
<tr>
<td>Domain - Set Domain - WF Activity Hist</td>
<td>wf_history</td>
<td>Sets the workflow activity history domain based on the parent workflow context's domain.</td>
</tr>
<tr>
<td>Domain - Set Domain - WF Context</td>
<td>wf_context</td>
<td>Sets the workflow context domain based on the referenced record's domain, if it has one.</td>
</tr>
<tr>
<td>Domain - Set Domain - WF Exec Activity</td>
<td>wf_executing</td>
<td>Sets the workflow executing activity domain based on the parent workflow context's domain.</td>
</tr>
<tr>
<td>Domain - Set task for - Change</td>
<td>change-request</td>
<td>When converting a ticket to a change request, sets the Requested by field to the ticket's Task for value.</td>
</tr>
<tr>
<td>Domain - Set task for - Incident</td>
<td>incident</td>
<td>When converting a ticket to an incident, sets the Caller field to the ticket's Task for value.</td>
</tr>
<tr>
<td>Name</td>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Domain - Validate Default</td>
<td>domain</td>
<td>Ensures only one domain has the Default check box selected.</td>
</tr>
<tr>
<td>Domain - Validate Primary</td>
<td>domain</td>
<td>Ensures only one domain has the Primary check box selected.</td>
</tr>
<tr>
<td>Business Rules Installed with Domain Support Plugin</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change Domain Set</td>
<td>sys_dictionary</td>
<td>Sets the domain set to the current domain.</td>
</tr>
<tr>
<td>Domain support properties</td>
<td>sys_properties</td>
<td>Sets the system properties to match the domain query method (domain paths or domain numbering).</td>
</tr>
</tbody>
</table>

**Client scripts**

<table>
<thead>
<tr>
<th>Client script</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain - Set Company and Location (sys_script)</td>
<td>Monitors the incident caller field for changes. If the company and location fields do not already have a value, the script adds this information from the caller record. If the company and location fields already have a value, the script retains the existing values.</td>
</tr>
<tr>
<td>Deactivated script</td>
<td></td>
</tr>
<tr>
<td>(BP) Set Location to User</td>
<td>Monitors the incident location field and sets the location field to the caller's location.</td>
</tr>
</tbody>
</table>

**Application support for domain separation**

Many ServiceNow applications support domain separation in the base system but not all. Some supported applications include limitations on the data and administrative settings that can be domain-separated. These definitions delineate the domain separation support levels from the perspective of actual use cases and the people who use them.

**Domain separation support levels**

ServiceNow applications that support domain separation may support the separation of data and data routing only, have advanced business logic separation, or support tenant (customer) level administration of the application. ServiceNow applications are defined with the following incremental support levels.
<table>
<thead>
<tr>
<th>Basic</th>
<th>Standard</th>
<th>Enhanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Data is domain-separated</td>
<td>• Application properties are domain-aware as needed</td>
<td>• Data-driven process enables failsafe configuration by tenants through the UI to drive business logic</td>
</tr>
<tr>
<td>• Logic exists to ensure proper data routing, caching, rollups, and aggregations</td>
<td>• Business logic can be domain-separated by the instance owner per tenant</td>
<td></td>
</tr>
<tr>
<td>• Global configuration operational for multiple tenants</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

No support

• The domain field may exist on data tables, but no logic exists to manage data.
• This level is not considered domain-separated.

Basic

• Business logic: Ensure data goes into the proper domain for the application’s service provider (SP) use cases.
• In the application, the user interface, cache keys, reporting, rollups, aggregations, and so on, all use domain at production run time.
• The owner of the instance needs to be able to set up the application to function across multiple tenants.

Use case: When an SP uses chat to respond to a tenant-customer’s message, the client must be able to see the SP’s response.

Standard

• Includes Basic level support.
• Business logic: Processes can be created or modified per customer by the service provider (SP). The use cases reflect proper use of the application by multiple SP customers in a single instance.
• The owner of the instance needs to be able to configure the minimum viable product (MVP) business logic and data parameters per tenant as expected for the specific application.

Use case: An admin needs to be able to make comments mandatory when a record closes for one tenant but not for another.

Enhanced

• Includes Basic and Standard levels
• Data-driven process enables service provider customers to modify business logic that is based on defined use cases. These configurations are UI-based and fail-safe so that configurations by one customer cannot affect another.
• Tenants of the instance need to be able to configure minimum viable product (MVP) business logic and data parameters for themselves. This logic and parameters would be expected for the application's normal function.

Use case: Tenant-customers of a shared environment need to be able to make changes to the impact, urgency, or priority matrix to set priority within their domain.

Note: Effective Domain (*)

• In some cases, a platform feature or application may effectively support SP use cases even without the domain framework. If so, the use cases must detail its support of domain separation. An asterisk (*) after the support level indicates this kind of configuration.

<table>
<thead>
<tr>
<th>Supported feature</th>
<th>Basic</th>
<th>Standard</th>
<th>Enhanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain column is present for base system application tables.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Domain-specific configuration is managed by instance owner.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Tenant domains can manage their own application data.</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Application properties are domain aware when needed.</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Business logic and processes can be domain-separated by instance owner.</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Business logic and processes can be administered by tenant domain.</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

Support levels by application

<table>
<thead>
<tr>
<th>Product Suite</th>
<th>Application</th>
<th>Support level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analytics, Intelligence, and Reporting</td>
<td>Dashboards</td>
<td>Basic</td>
</tr>
<tr>
<td></td>
<td>Performance Analytics</td>
<td>Enhanced</td>
</tr>
<tr>
<td></td>
<td>Process Optimization</td>
<td>Basic</td>
</tr>
<tr>
<td></td>
<td>Reporting</td>
<td>Basic</td>
</tr>
<tr>
<td></td>
<td>User Experience Analytics</td>
<td>No support</td>
</tr>
<tr>
<td>Custom Business Applications</td>
<td>Delegated Development</td>
<td>No support</td>
</tr>
<tr>
<td></td>
<td>ODBC Driver</td>
<td>Basic*</td>
</tr>
<tr>
<td></td>
<td>Script debugger</td>
<td>Basic</td>
</tr>
<tr>
<td></td>
<td>Web Services</td>
<td>Standard*</td>
</tr>
<tr>
<td>Customer Service Management</td>
<td>Communities</td>
<td>No support</td>
</tr>
<tr>
<td>Product Suite</td>
<td>Application</td>
<td>Support level</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Customer Service Management</td>
<td></td>
<td>Basic</td>
</tr>
<tr>
<td>Employee Service Management</td>
<td>HR Service Delivery</td>
<td>Basic*</td>
</tr>
<tr>
<td></td>
<td>Legal Service Delivery</td>
<td>Basic</td>
</tr>
<tr>
<td></td>
<td>Safe Workplace Suite</td>
<td>See site for individual application support levels</td>
</tr>
<tr>
<td>Field Service Management</td>
<td>Field Service Management</td>
<td>Basic</td>
</tr>
<tr>
<td>Financial Services Operations</td>
<td>Financial Services Card Operations</td>
<td>Basic</td>
</tr>
<tr>
<td></td>
<td>Financial Services Payment Operations</td>
<td>Basic</td>
</tr>
<tr>
<td>Governance, Risk, and Compliance</td>
<td>Governance, Risk, and Compliance (GRC)</td>
<td>Basic</td>
</tr>
<tr>
<td>IT Asset Management</td>
<td>Hardware Asset Management</td>
<td>Enhanced</td>
</tr>
<tr>
<td></td>
<td>Software Asset Management</td>
<td>Enhanced</td>
</tr>
<tr>
<td>IT Business Management</td>
<td>Agile Development</td>
<td>Basic*</td>
</tr>
<tr>
<td></td>
<td>Application Portfolio Management</td>
<td>Basic</td>
</tr>
<tr>
<td></td>
<td>Cost Management</td>
<td>No support</td>
</tr>
<tr>
<td></td>
<td>Demand Management</td>
<td>Basic</td>
</tr>
<tr>
<td></td>
<td>Financial Management</td>
<td>No support</td>
</tr>
<tr>
<td></td>
<td>Investment Funding</td>
<td>Basic</td>
</tr>
<tr>
<td></td>
<td>Project Portfolio Management</td>
<td>Basic*</td>
</tr>
<tr>
<td></td>
<td>Release Management</td>
<td>Basic*</td>
</tr>
<tr>
<td></td>
<td>Scaled Agile Framework (SAFe)</td>
<td>Basic*</td>
</tr>
<tr>
<td></td>
<td>Test Management</td>
<td>Basic*</td>
</tr>
<tr>
<td>IT Operations Management</td>
<td>Cloud Provisioning and Governance</td>
<td>Basic</td>
</tr>
<tr>
<td></td>
<td>Discovery</td>
<td>Standard</td>
</tr>
<tr>
<td></td>
<td>Event Management</td>
<td>Basic</td>
</tr>
<tr>
<td></td>
<td>Health Log Analytics</td>
<td>No support</td>
</tr>
<tr>
<td></td>
<td>Operational Intelligence</td>
<td>Basic</td>
</tr>
<tr>
<td></td>
<td>Service Mapping</td>
<td>Basic</td>
</tr>
<tr>
<td>IT Service Management</td>
<td>Benchmarks</td>
<td>No support</td>
</tr>
<tr>
<td></td>
<td>Change Management</td>
<td>Basic</td>
</tr>
<tr>
<td></td>
<td>Coaching</td>
<td>Basic</td>
</tr>
<tr>
<td></td>
<td>Continual Improvement Management</td>
<td>Basic</td>
</tr>
<tr>
<td></td>
<td>Contract Management</td>
<td>No support</td>
</tr>
<tr>
<td></td>
<td>Expense Line</td>
<td>No support</td>
</tr>
<tr>
<td></td>
<td>Incident Communications Management</td>
<td>Standard</td>
</tr>
<tr>
<td></td>
<td>Facilities Service Management</td>
<td>Standard</td>
</tr>
<tr>
<td></td>
<td>Incident Management</td>
<td>Standard</td>
</tr>
<tr>
<td>Product Suite</td>
<td>Application</td>
<td>Support level</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
<td>---------------</td>
</tr>
<tr>
<td></td>
<td>On-Call Scheduling</td>
<td>Standard</td>
</tr>
<tr>
<td></td>
<td>Problem Management</td>
<td>Standard</td>
</tr>
<tr>
<td></td>
<td>Procurement</td>
<td>Standard*</td>
</tr>
<tr>
<td></td>
<td>Product Catalog</td>
<td>Standard</td>
</tr>
<tr>
<td></td>
<td>Request Management</td>
<td>Standard</td>
</tr>
<tr>
<td></td>
<td>Service Catalog</td>
<td>Standard</td>
</tr>
<tr>
<td></td>
<td>Service Desk Call</td>
<td>Basic</td>
</tr>
<tr>
<td></td>
<td>Service Level Management</td>
<td>Standard</td>
</tr>
<tr>
<td></td>
<td>Service Portfolio Management</td>
<td>Basic*</td>
</tr>
<tr>
<td></td>
<td>Vendor Performance</td>
<td>No support</td>
</tr>
<tr>
<td></td>
<td>Walk-up Experience</td>
<td>Basic</td>
</tr>
<tr>
<td>Mobile Configuration and Navigation</td>
<td>Mobile</td>
<td>Basic</td>
</tr>
</tbody>
</table>

### Now Platform:

<table>
<thead>
<tr>
<th>Application</th>
<th>Support level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration, App Engine, Capabilities, and User Interface</td>
<td></td>
</tr>
<tr>
<td>Advanced Work Assignment</td>
<td>Standard</td>
</tr>
<tr>
<td>AI Search</td>
<td>Searches respect domain restrictions from indexed Now Platform records</td>
</tr>
<tr>
<td>App Engine Studio</td>
<td>No support</td>
</tr>
<tr>
<td>Assessments</td>
<td>Standard</td>
</tr>
<tr>
<td>Automated Test Framework</td>
<td>Standard*</td>
</tr>
<tr>
<td>Connect Support and Chat</td>
<td>Basic</td>
</tr>
<tr>
<td>Contextual Search</td>
<td>Standard</td>
</tr>
<tr>
<td>Configuration Management (CMDB)</td>
<td>Standard</td>
</tr>
<tr>
<td>Content Management System</td>
<td>No support</td>
</tr>
<tr>
<td>Credentials and Connections</td>
<td>Standard</td>
</tr>
<tr>
<td>Data Certification</td>
<td>Basic*</td>
</tr>
<tr>
<td>Data Classification</td>
<td>Enhanced</td>
</tr>
<tr>
<td>Data Management</td>
<td>Basic*</td>
</tr>
<tr>
<td>Dependency Views</td>
<td>Basic</td>
</tr>
<tr>
<td>Dynamic Translation</td>
<td>Basic</td>
</tr>
<tr>
<td>Edge Encryption</td>
<td>No support</td>
</tr>
<tr>
<td>Encryption Support</td>
<td>No support</td>
</tr>
<tr>
<td>Field Normalization</td>
<td>No support</td>
</tr>
<tr>
<td>Flow Designer</td>
<td>Standard*</td>
</tr>
<tr>
<td>Guided Setup</td>
<td>No support</td>
</tr>
<tr>
<td>Homepage Administration</td>
<td>Basic*</td>
</tr>
<tr>
<td>IntegrationHub</td>
<td>Standard*</td>
</tr>
<tr>
<td>Product Suite</td>
<td>Application</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Integrations with third-party applications and data sources</td>
</tr>
<tr>
<td></td>
<td>Knowledge Management</td>
</tr>
<tr>
<td></td>
<td>Managed Documents</td>
</tr>
<tr>
<td></td>
<td>MetricBase</td>
</tr>
<tr>
<td></td>
<td>Notifications</td>
</tr>
<tr>
<td></td>
<td>Orchestration</td>
</tr>
<tr>
<td></td>
<td>Password Reset</td>
</tr>
<tr>
<td></td>
<td>Platform Security</td>
</tr>
<tr>
<td></td>
<td>Predictive Intelligence</td>
</tr>
<tr>
<td></td>
<td>Process Automation Designer</td>
</tr>
<tr>
<td></td>
<td>Remote Tables</td>
</tr>
<tr>
<td></td>
<td>Schedules</td>
</tr>
<tr>
<td></td>
<td>Search Suggestions</td>
</tr>
<tr>
<td></td>
<td>Service Portal</td>
</tr>
<tr>
<td></td>
<td>State Flows</td>
</tr>
<tr>
<td></td>
<td>Subscription Management</td>
</tr>
<tr>
<td></td>
<td>Survey Management</td>
</tr>
<tr>
<td></td>
<td>Time Card</td>
</tr>
<tr>
<td></td>
<td>UI Builder</td>
</tr>
<tr>
<td></td>
<td>Virtual Agent</td>
</tr>
<tr>
<td></td>
<td>Visual Task Boards</td>
</tr>
<tr>
<td></td>
<td>Workflow</td>
</tr>
<tr>
<td></td>
<td>Workspace</td>
</tr>
<tr>
<td></td>
<td>IBM QRadar Offense Ingestion</td>
</tr>
<tr>
<td></td>
<td>Microsoft Graph Security API alert ingestion integration</td>
</tr>
<tr>
<td></td>
<td>Security Incident Response</td>
</tr>
<tr>
<td></td>
<td>Threat Intelligence</td>
</tr>
<tr>
<td></td>
<td>Trusted Security Circles</td>
</tr>
<tr>
<td></td>
<td>Vulnerability Response</td>
</tr>
<tr>
<td></td>
<td>Coaching Loops (Legacy)</td>
</tr>
<tr>
<td></td>
<td>Finance Service Management</td>
</tr>
<tr>
<td></td>
<td>Planned Maintenance</td>
</tr>
<tr>
<td></td>
<td>Structured Problem Analysis</td>
</tr>
<tr>
<td></td>
<td>Order Management</td>
</tr>
<tr>
<td></td>
<td>eBonding for Telecommunications</td>
</tr>
<tr>
<td></td>
<td>Service Portal</td>
</tr>
<tr>
<td></td>
<td>State Flows</td>
</tr>
<tr>
<td></td>
<td>Subscription Management</td>
</tr>
<tr>
<td></td>
<td>Survey Management</td>
</tr>
<tr>
<td></td>
<td>Time Card</td>
</tr>
<tr>
<td></td>
<td>UI Builder</td>
</tr>
<tr>
<td></td>
<td>Virtual Agent</td>
</tr>
<tr>
<td></td>
<td>Visual Task Boards</td>
</tr>
<tr>
<td></td>
<td>Workflow</td>
</tr>
<tr>
<td></td>
<td>Workspace</td>
</tr>
<tr>
<td></td>
<td>IBM QRadar Offense Ingestion</td>
</tr>
<tr>
<td></td>
<td>Microsoft Graph Security API alert ingestion integration</td>
</tr>
<tr>
<td></td>
<td>Security Incident Response</td>
</tr>
<tr>
<td></td>
<td>Threat Intelligence</td>
</tr>
<tr>
<td></td>
<td>Trusted Security Circles</td>
</tr>
<tr>
<td></td>
<td>Vulnerability Response</td>
</tr>
<tr>
<td></td>
<td>Coaching Loops (Legacy)</td>
</tr>
<tr>
<td></td>
<td>Finance Service Management</td>
</tr>
<tr>
<td></td>
<td>Planned Maintenance</td>
</tr>
<tr>
<td></td>
<td>Structured Problem Analysis</td>
</tr>
<tr>
<td></td>
<td>Order Management</td>
</tr>
<tr>
<td></td>
<td>eBonding for Telecommunications</td>
</tr>
</tbody>
</table>
Domain separation recommended practices for service providers

You can create, implement, and maintain domain separation for your applications and services.

Domain basics

With domain separation (also known as ServiceNow Multitenant Platform Architecture), you can segregate the application data, user interface, and business logic in a single customer instance that supports hierarchical modeling with cross-tenant intelligence. Business logic describes how the domain separation is configured and what rules are affecting the configuration.

Before you set off on the domain separation journey, here are some good practices to follow. Select topics as you want or follow them in order by clicking the links below the image.
Domain separation explained

With domain separation, you can segregate application data, UI, and business logic, such as rules or workflows, in a single customer instance. Separating these elements into logically defined domains supports specific hierarchies for all customers using your applications.

Domain basics

Domain separation, also known as ServiceNow multitenant platform architecture, adds considerable overhead to the management of an instance. If you use domain separation correctly though, it can improve efficiency, add greater security, and increase the performance of your customers' instances.

You can't separate some global standards and properties, such as system properties and table schema, per tenant.

Before you start separating domains, read the following guidelines.

What you can do with domain separation

- Data separation: Enables tenants of the domain to see only data that they have permissions to see. Tenants can be granted access to other tenant data but can't query tenant data that they don't have access to.
  - When you update data records, they do not generate Update Set records.
  - Users, including the customer accounts that are used for integrations, see only the data in the domains they have permission to access.
  - Customers, agents, and fulfillers see data that pertains to the customers and organizations that they support.
- UI separation: Supports a tenant-specific experience for UI elements such as views, lists, labels, and so on.
  - You can override the browser-based user interface, including application menus, lists, forms, homepages, and dashboards. You can also customize them for a specific domain or set of domains while preserving your basic process logic.
  - Service providers can alter the displayed branding and UI elements to meet individual customer needs.
- Business logic separation: Creates tenant-specific system policies such as email notifications, business rules, client scripts, UI policy, and UI actions.
- Hierarchical modeling: Nests your multiple tenants so that parent tenants can access child tenant resources.
  - Business logic for parent tenants runs automatically for child tenants, which you can override at any level.
- Cross-tenant intelligence: Automatically handles data, metadata, business logic, and processing context for tenants with access to additional tenant data.

Domain separation at a glance

The following graphic shows the division of data, process, and UI separation. These concepts are discussed in depth in the Recommended Practices section.
Domain Separation

Ability to establish sub-tenants (logically defined domains) within a single ServiceNow instance

Data Separation

Process Separation

UI Separation

Global Standards, Centralized Administration, and Reporting

Domain architecture

User records are assigned a domain value that represents the user’s home domain. Users have no access to data in parent domains, peer domains, or domains in other branches of the hierarchy.

See Contains queries and domain access for advanced options to grant additional domain visibility.

The following diagram shows how the architecture process flows down to the child domains.
Domain separation value proposition
With domain separation, service providers can have a multitenant instance architecture that delivers offerings efficiently and securely to their clients. Strong universal process standards, data-driven process design, strict governance, and centralized administration help to maximize these benefits.
**Benefits of domain separation**

The tenants of a domain benefit from a quick return on investment, lower administrative overhead, and leverage of business services provided by instance owners.

Here is a quick view of these benefits.

<table>
<thead>
<tr>
<th>Instance Owner</th>
<th>Domain Tenants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service provider employee productivity</td>
<td>Increased security</td>
</tr>
<tr>
<td>Only process deltas maintained</td>
<td>Pre-built processes and features</td>
</tr>
<tr>
<td>Administration efficiencies</td>
<td>Reduced staff required</td>
</tr>
<tr>
<td>Fewer client integrations</td>
<td>Faster onboarding</td>
</tr>
<tr>
<td>Upgradability and scalability</td>
<td>Leverage of the latest releases</td>
</tr>
<tr>
<td>Data segregation</td>
<td>Services provided by the instance owner</td>
</tr>
<tr>
<td>Global reporting</td>
<td></td>
</tr>
</tbody>
</table>

**Definition of domain separation**

With domain separation (also known as the ServiceNow® Multitenant Platform Architecture), you can segregate application data, UI, and business logic in a single customer instance that supports hierarchical modeling with cross-tenant (customer) intelligence.

**Properties of domain separation**

Domain-separated ServiceNow applications are defined with the following properties:

**Data separation**

Enables customers to see only the data that they have permissions to see. Customers can be granted access to other customer data but cannot query customer data if they don't have access.

**UI separation**

Supports a customer-specific experience for UI elements such as views, lists, labels, and so on.

**Business logic separation**

Supports customer-specific system policies such as email notifications, business rules, client scripts, UI policy, and UI actions.

**Hierarchical modeling**

Supports nested-multitenancy so parent tenants (customers) can access child customer resources. The business logic for parent customers runs automatically for child customers and can be overridden at any level.

**Cross-customer intelligence (domain scope)**

Handles automatically the data, metadata, business logic, and processing context for tenants that have access to additional tenant data.
How domain separation works
A common analogy for understanding how domain separation works is by looking at a comparison of a single-family home (single-tenant) versus an apartment complex (domain-separated).

**Single-family home vs. apartment complex**

With a house, you pay more but you get more control. You can knock down walls, paint, add a room or pool, and so on.

With an apartment complex, someone else decides all of those things for you. Sometimes, you can't even paint the walls that you live within.

**Single versus multiple tenants**

**Single-tenant instance**

You're a ServiceNow customer, you bought the licenses, and it's up to you to decide what services you want. You can upgrade when you want, see previews of all the great new features, and configure your instance right away. Being a single tenant has these benefits and restrictions:

- You have higher upfront costs and administrative overhead, but you have more freedom to remodel and expand.
- You have higher costs to obtain and maintain the instance and supply administration staff. Although you are free to build out the environment as required, you must comply with the ServiceNow recommended practices and standards.

**Multiple-tenant instance**

Someone else owns the instance, possibly a service provider with multiple customers. They upgrade when they want and put new services on the instance when they want. If you are a customer of a service provider, you are most likely on their instance because you wanted what they offer. Multiple tenants have these benefits and restrictions:

- A centralized staff administers configurations, integrations, and upgrades.
- The instance owner provides added services.
- Domain tenants have lower upfront costs to use the ServiceNow platform, have lower monthly costs because they are sharing it with many tenants, and do not have to employ a staff to administer the environment.
- Benefits shared from requests or changes that are initiated by other tenants.

**Analogy summary**

<table>
<thead>
<tr>
<th>Domain separation attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Single-family home</strong></td>
</tr>
<tr>
<td>Mortgage</td>
</tr>
<tr>
<td>Owner responsible for maintenance / utilities</td>
</tr>
<tr>
<td>Can remodel and expand</td>
</tr>
<tr>
<td>Compliance with zoning laws</td>
</tr>
</tbody>
</table>
Domain separation hierarchies

Create a hierarchy when defining a domain architecture to track your processes and workflows.

Sample domain separation hierarchies

The following diagram suggests a good starting point for defining domain architecture. It demonstrates the relationship between the TOP and lower domains and how the process, data, and business rules impact parent and child domains.

- In the following example, TOP is a process domain. It should never contain users. TOP should contain the new processes that instance owners develop and the overrides to these processes from the global domain.
- Only the service provider (SP) has access to the default domain. This domain never contains active users. It contains only the lost data that you need to reassign to the correct domain.

**Note:** When data is not assigned to a specific domain, it goes to the default domain. It is temporarily "lost" and needs to be assigned to its correct domain.

- Tasks and users without a domain are placed in the default domain automatically when you create or update domains. You can override this behavior by either clearing the Default option on this record or selecting the Default option on another domain record. If you have not set a default domain yet, tasks and users with no domain are placed in the global domain.
- Don't move data between domains when you are using the instance.
- If any data ends up in the default domain, that means you have a configuration or procedural problem to address.

- You don't see the word "Global" in this diagram because there is no global domain; "Global" is the absence of a domain on a record.
- For example, a table that has no domain field means that the table contains all global records. A table that has a domain field means that any record without a domain is a global domain.
- The word "Global" is in the domain field. It is placed there automatically when the record has no domain.
- Global records are available to all users of the instance unless they are restricted by security configurations.
- Use the default domain to make sure that records do not end up in the global domain on tables that should never have global records.
- Instance owners must then triage the records in the default domain and move them to the correct domain.
Domain hierarchies

- Parent/child – Process and data affected
  - Design that is based on a process flow. Remember that the parent domains can access all data in the child domains.
• "Contains" domain – Only data is affected. For example, making SP in the diagram contain TOP does not make processes in SP run in the TOP domain and downward.
  • Grants data access rights to individuals in groups that require dedicated access to certain domains.
  • Contains causes or conditions to be added to DB queries that can cause performance issues with large domain and data sets.

• Visibility – Hierarchy that is always visible to users once you provide access. Only the data is affected, not the processes.
  • Grants data access of a domain to another domain that did not have that access when the parent and child hierarchy was built.
  • Enables users to see all the data in the domains that they are granted visibility to, all the time, regardless of the record they are working on.

**Note:** Use sparingly, as it can allow complete access that you may not intend.

Many SPs have customers who implicitly state that access to their domains must be tightly regulated, which constrains the use of “Contains” at the TOP domain. The following diagram explains how to mitigate that regulation by dividing domains into Restricted and Unrestricted domains.
Unrestricted and restricted use cases for domain separation

Here is how to handle such cases:

- Under TOP, create two domains, Unrestricted and Restricted.
  - For customers who do not have SP visibility restraints, place those customers and their domains under Unrestricted.
  - For customers who do have that requirement, place them and their domains under Restricted.
- System admins can then use “Contains” and “Visibility” functions in an efficient, targeted manner.
  - Apply "Contains" to Unrestricted, so a single “Contains” can grant visibility to most customers.
  - Apply domain visibility using ”domain visibility groups” to specific domains as needed.

Tasks and users without a domain are placed in this domain when created or updated. You can override this behavior by:

1. Clearing the Default option on this record.
2. Selecting the Default option on another domain record.

If no domain is set as default, tasks and users that have no domain are placed in the Global domain.
The following diagram delineates how to choose which hierarchy model is right for you. You can choose separate hierarchies, hybrid, or shared hierarchies depending on which processes and functionality you want in your domain structures.

Customer Decision Trees

Partner Sales uses tree to determine if a new customer should directly interact with managed instance or dedicated instance.

Customer installs the service providers CONNECTOR directly off the Store which allows customer to connect to the service providers managed instance for consumption of service(s).

Customer wants NOW for reasons other than the providers services.

See Dedicated vs. Shared tree for detail on this step.

Provider sells NOW licenses, sells/outsources professional services, and deploys CONNECTOR on the customer’s instance.

Provider sells fully managed service delivered in domain-separated instance. Customer doesn’t want ServiceNow platform, but does want its user experience for service(s) purchased.
Context and domain separation

The context of a user's session determines the processes, data, and user interface (UI) as the user browses through list views, home pages, reports, and knowledge articles. The context is determined by the processes that you create, the business rules that you set, your workflows, and other factors.

User session context

Many factors determine the context of a user session, such as user profiles, groups, company criteria, and so on. In the following diagram, you see that the incidents that a company has created are part of the context.

The user in this example has a home domain of Cloud Dimensions.

1. The branding reflects the settings in the Cloud Dimensions domain and company record.
2. The application navigator shows the items that are inherited from higher-level domains as well as the modules that are defined in the Cloud Dimensions domain.
3. The home pages and list data reflect the data that is visible to the user. This data is based on the user’s session context. In this case, the user in the Cloud Dimensions domain can see the data in Cloud Dimensions, child domains, and the global domain.

**User session context starts in the home domain**

In the following diagram, you can see the elements of the context.

![Diagram showing user session context](image)

The system administrator sets users' home domains on their user records. Typically, a user’s home domain is set to the same domain as their company’s domain. When the user logs in, the domain picker sets automatically to the user’s home domain. Users can return to their home domain at any time by clicking the arrow icon on the domain picker.

The domain picker's list includes domains within the user’s session context. Users may further limit their session context by selecting child domains with the picker.

The context of the user session includes the user’s home domain and any child domains. This set of domains in the user’s session context is appended automatically to every query that is sent to the database. That way, the results are limited to just the data in these domains and global data. This process is embedded in the compiled code that is not accessible.

Service accounts that are used for integrations also have user session context. There is user context and records context, each with its own data in its own domain. These contexts affect the integrations. Database queries (records) are limited in the same way as interactive users (users), meaning that they work as normal but are limited by whatever constraints the developer has configured.

You can learn about additional ways to add domains to a user’s session context in Service provider reference architecture.
Record context

As a user drills into individual records, record context is activated. The record context determines the UI elements and processes to apply to the record.

A record’s domain dictates the process, data, and the availability of UI elements within the record.

Note:

• Record context persists even if the user's domain changes.
• Users can view records concurrently in multiple browser tabs, while maintaining their own record context.
Segregating and securing data with domain separation

You can segregate and secure data on the ServiceNow platform in multiple ways, depending on your customer's needs.

Segregating data in multiple ways

The following diagram shows four ways that you can segregate data. You can use separate instances, domain separation, contextual security and business rules, and the reference architecture itself as ways to segregate data.

You can segregate data in these four ways:

1. Customizing the reference architecture with qualifiers and filters so that departments and groups within a company can focus on their own work. By segregating the data between these departments or groups, a department or group can't see another department or group's records.

2. Adding contextual security and Before Query business rules as additional layers of security to guard against data breaches. See Context and domain separation and Before Query business rules to learn more about domain separation and business rules.

3. Adding another level of security in a company by using domain separation. The data from every database query is limited to the data that is visible in a domain before contextual security and business rules are executed.

4. Using separate instances to segregate the data at the database and application layer.
Separate instances, domain separation, contextual security and business rules, and the reference architecture are ways to segregate data. These four ways relate to each other as indicated by the Comprehensiveness of need arrow in the diagram. How each layer interacts with the other layers depends on how you set up your domain separation configuration.

Not all organizations require domain separation. You might find other alternatives, such as separate instances or a single instance without a domain. To learn more about these alternatives, see Evaluating the need for domain separation.

Alternatives to domain separation

You can use a separate instance as an alternative to domain separation for your customers. A separate instance allows you the flexibility to meet the requirements for data separation within the groups and departments in an organization with little to no impact on others.

Separate instances

Pros and cons of separate instances

<table>
<thead>
<tr>
<th>Separate instance</th>
<th>Single instance - without domain</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pros</strong></td>
<td><strong>Pros</strong></td>
</tr>
<tr>
<td>Built to suit each customer/organization</td>
<td>May address simple scenarios</td>
</tr>
<tr>
<td>Minimize impact of customization on others</td>
<td>Cost</td>
</tr>
<tr>
<td>Release schedule coordination</td>
<td><strong>Cons</strong></td>
</tr>
<tr>
<td>Clean separation</td>
<td>Extensive modifications to baseline code</td>
</tr>
<tr>
<td>Choose DATACENTER region</td>
<td>Modified base system code skipped during upgrades</td>
</tr>
<tr>
<td><strong>Cons</strong></td>
<td>Must address all secondary and supporting tables as well</td>
</tr>
<tr>
<td>Cost</td>
<td>Extensive testing required</td>
</tr>
<tr>
<td>Alignment of instances</td>
<td>No ServiceNow product team to evolve your custom code</td>
</tr>
<tr>
<td>Testing effort for upgrades</td>
<td></td>
</tr>
<tr>
<td>Duplication of effort</td>
<td></td>
</tr>
<tr>
<td>Integrations required</td>
<td></td>
</tr>
</tbody>
</table>

You can time upgrades and releases separately for each instance. However, if you choose to use separate instances, you need to do a lot of coordination with other people who are administering instances. By configuring an instance with contextual security, form views, reference qualifiers, filters, and robust conditions, you don't have to use domain separation in your company.

With a separate instance, you may address data and process separation but your instance owners must maintain and keep up with the extensive customizations that is required for separate instances.

Evaluating the need for domain separation

You may find that domain separation doesn't always work for your customers' organizations. It's best that you base your decision to go with domain separation by looking at your customers' needs.
Reasons for domain separation

These factors may help you decide to choose domain separation for your customers' organizations:

- Your customers have moderate alignment of processes and general platform requirements.
- Your customers plan to work on tasks as fulfillers rather than as requesters.
- Your customers have a contractual agreement that requires that data records be isolated, but your instance owner has determined that the requirement may be addressed somewhere else in the configuration.
- Your company's instance owners have entire entities that operate as physically separate organizations and do not share data, but full reporting is still required. Separate domains would allow data visibility when configured correctly.

Reasons for no domain separation

These factors can point to reasons why your customers' organizations might not want to set up domain separation:

- Your customers want to administer their environment, have full ownership of it, and set the roadmap for expansion.
- Your customers require that the data and process at the physical or database level be completely isolated.

Note:

Domain-separated instances contain a shared database so this undermines the isolation requirement.

- Departments in your customers' organization want to isolate records. (Access controls may suffice.)
- Your customers all want their own processes, business rules, and workflows.
- The corporate culture is one of non-collaboration between your customers' organizations.
- Your customers interact with the platform as end users only.
Benefits of domain separation

Domain separation may work better for your customers' organizations than any other method for separating the data between groups and departments.

Domain separation benefits at a glance

You can enable domain separation with a ServiceNow plugin that has functionality built into the core platform. The separate domains configuration is managed by a product manager who is supported by a development team. Enhancements and fixes for domain separation functionality are included with ServiceNow releases and ready to be used by customers. For assistance with domain separation, your instance owners can use Customer Service and Support resources, such as the Service Portal.
How a database query works with domain separation

Using database queries with domain separation in your customers' applications help them protect their data. These queries then speed up the configuration and build processes.

How domain separation protects data

In the following figure, the Incident table [incident] has a domain field that is inherited from the incident's task. When you see this domain field, you know that the records in the table can have domain assignments.

When users log in, their home domain appears with the set of domains they may access. This is known as the user’s session context. For more information about session contexts, see Context and domain separation.
1. In a browser, the user from one of the companies, Acme, selects the Open Incidents module to view all incidents where active=true.

2. The active=true filter is submitted to the application.

3. The application then sends a query to the database by appending a WHERE clause to active=true. The WHERE clause limits the incident records that are returned to those records that are in the user's domain or the domains that the user may access. Only the records in these domains are returned to the application for processing.
4. Contextual security is applied, further limiting the data that is returned to the user. The incident records appear in the Open Incidents list.

**Note:**

When you apply contextual security, you create limits to the data that are returned to the user. These limits protect other content that you may not want users to see.

To learn more about contextual security, see *Context and domain separation.*

**Note:** This processing logic applies for all queries to the database, including those queries that are triggered using integrations.

### Domain separation levels of support

You can choose from three high-level categorizations for domain separation of an application for your customers' organizations. Applications that support domain separation may support the separation of data and data routing only, have advanced business logic separation, or support tenant (customer) level administration of the application. These definitions delineate the support levels from the perspective of actual use cases and the people who implement them.

### Incremental ServiceNow support levels

<table>
<thead>
<tr>
<th>Level</th>
<th>Type</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>No support</td>
<td></td>
<td>• The domain field may exist on data tables, but no business logic exists to manage the data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• This level is not considered domain-separated.</td>
</tr>
<tr>
<td>Level</td>
<td>Type</td>
<td>Summary</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Basic</td>
<td>Customer data management</td>
<td>• Business logic: Ensures that data goes into the proper domain for the application’s service provider use cases.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• In the application, user interface, cache keys, reporting, rollups, aggregations, and so on, all consider the properties of the domain at run time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Your instance owners need to be able to set up the application to function normally across multiple tenants.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use case: When a service provider uses chat to respond to a customer’s message, the client must be able to see the response.</td>
</tr>
<tr>
<td>Standard</td>
<td>Customer process management</td>
<td>• Includes the Basic level</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Business logic: Processes can be created or modified per customer by the service provider. The use cases reflect how the application is used by multiple service provider customers in a single instance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Your instance owners need to be able to configure minimum viable product (MVP) business logic and data parameters per customer for the specific application.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use case: Admin needs to be able to make comments required when a record closes for one customer, but not for another customer.</td>
</tr>
<tr>
<td>Enhanced</td>
<td>Customer self-managed configuration</td>
<td>• Includes Basic and Standard levels</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enables service provider customers to modify business logic that is based on defined use cases. These configurations are UI-based and fail-safe so that configurations by one customer cannot affect another customer.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The instance customers need to be able to configure MVP business logic and data parameters themselves.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use case: Customer of a shared environment needs to be able to make changes according to impact, urgency, or priority within a domain.</td>
</tr>
</tbody>
</table>
Effective domain*

In some cases, a platform feature or application may support service provider use cases even if the domain framework is not being used. The use cases must be detailed to support domain separation. An asterisk (*) after the support level indicates this kind of configuration.

Use case: Before the New York release, Service Catalog had no domain support but the instance owners could configure separate catalogs and items for each tenant in a domain-separated instance by using user criteria. The result was that each tenant could use Service Catalog at a Standard level.

To view all applications listed by their support level see Application support for domain separation.

Summary

Domain separation is a framework that you must use to make your applications aware of its customers.

Consider the domain framework capabilities, your applications' business use cases, what the personas are, and how they use the application before you can use the framework to make your application supportable.

Service provider reference architecture

Your customers can access service provider (SP) services by using a portal that is designed for them to reach their domain-separated instance.

Basic attributes of service provider reference architecture

- You do not assign fulfillers to a domain. Instead, you share them across domains. This makes it harder to audit how many fulfillers you have per domain.
- You can share and leverage domain administration. This means that there is no overhead and you can optimize licenses.
- The number of users on the instance can change when you get a new customer. A new customer can result in tens or even hundreds of thousands of new users on the system. The number of total users is virtually unlimited in one shared environment.
The portal for SP services is dedicated or shared to the SP shared instance. Service providers use ServiceNow shared instances to manage their service delivery.
Reference hierarchy for domain-separated instances

- **SP Contains TOP**
  - Service provider (SP)
    - Domain contains TOP for complete data access.
  - TOP
    - Top-level, process flows down
    - Overrides from global processes are done here.

- **Parent/Child**
  - SP “Contains” TOP
    - For complete data access
  - Initex
    - Can access only from global and itself
  - Oceanic Airlines
    - Can access only from global and itself
  - ACME
    - Can access only from global and itself
  - Cisco
    - Example 3rd-party vendor
You can use decision trees and a comparison chart to determine if a new customer should be added to a shared instance or to their own dedicated instance.

**Decision trees**

Use these decision trees to help your customers decide whether to use a managed or dedicated instance.
Customer decision tree
## SP reference architecture comparison

<table>
<thead>
<tr>
<th>Standalone (SA)</th>
<th>Multi-Tenant (MT)</th>
<th>Hybrid (MT+SA)</th>
<th>SIAM (Multi-Vendor)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Platform as a Service</strong></td>
<td><strong>Enterprise scale</strong></td>
<td><strong>Processes simplified</strong></td>
<td><strong>Cost reduction</strong></td>
</tr>
<tr>
<td>Customer wants full power of platform to solve own needs outside those offered by SP.</td>
<td>Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.</td>
<td>Global governance &amp; admin for business use case &amp; process can be developed &amp; maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.</td>
<td>Lower administration, transaction, &amp; onboarding costs, &amp; ongoing operational costs for resources &amp; licensing. Faster onboarding = more revenue.</td>
</tr>
</tbody>
</table>
Service provider reference architecture for dedicated instances
Service provider (SP) customers can access SP services by using a portal to a dedicated instance. SPs use these dedicated instances to manage their service delivery.

Dedicated instances

- SP customers access SP services via a portal to a dedicated instance
- SP uses dedicated instance(s) to manage their service delivery

Legend:
- Centralized governance at the SP for instances managed by the SP
- Administration owned by the SP or customer for dedicated instances
- SP & customer fulfillers on each instance
- Customer requesters on each instance

Attributes

- Dedicated instances require that you have separate administration and dedicated teams. You need multiple licenses for the administrators and developers who log in to multiple instances.
- Each instance has a finite number of requesters and fulfillers. When you get a new customer, you must procure an instance that is based on the size and scale of your customer’s company.
Dedicated instance

Legend:
- Centralized governance at the SP for instances managed by the SP
- Administration owned by the SP or customer for dedicated instances
- SP & customer fulfillers on each instance
- Customer requesters on each instance

- SP customers access SP services via a portal to a dedicated instance
- SP uses dedicated instance[s] to manage their service delivery
Dedicated vs. shared instance
### SP reference architecture comparison

**Service provider reference architecture for hybrid**

Use the hybrid service provider (SP) reference architecture for a customized solution. Your customers require a dedicated instance for a specific service. They can still use the shared SP instance for other services, but it requires integration of each instance.

### Hybrid architecture

Your customer may be responsible for delivering this additional service directly. You’ll need to build a hybrid solution of several attributes for your customer to provide.
Attributes

- You can share and leverage the administration of the instance. This means that there is no overhead, and you can optimize licenses.
- If there is a new instance for a decentralized environment, the program team is responsible and funded accordingly as dedicated administrator users for that instance. In a centralized environment where all instances stem from a blueprint, you'll need duplicate administration licenses.
- You do not assign fulfillers to a domain. Instead, you can share them across domains.
- If a customer is sharing both a shared environment and a dedicated environment, they require a filler in both environments. This means more work for each team because the processes for shared and dedicated instances require different work for each instance.
- The number of users on the instance can change when you get a new customer. A new customer can result in tens or even hundreds of thousands of new users on the system. The number of total users is virtually unlimited in one shared environment.
Each instance has a finite number of requesters and fillers. When you get a new customer, you must procure an instance that is based on the size and scale of your customer's company.

<table>
<thead>
<tr>
<th>Standalone (SA)</th>
<th>Multi-Tenant (MT)</th>
<th>Hybrid (MT+SA)</th>
<th>SIAM (Multi-Vendor)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform as a Service</td>
<td>Enterprise scale</td>
<td>Processes simplified</td>
<td>Cost reduction</td>
</tr>
<tr>
<td>Customer wants full power of platform to solve own needs outside those offered by SP.</td>
<td>Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.</td>
<td>Global governance &amp; admin for business use case &amp; process can be developed &amp; maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.</td>
<td>Lower administration, transaction, &amp; onboarding costs, &amp; ongoing operational costs for resources &amp; licensing. Faster onboarding = more revenue.</td>
</tr>
</tbody>
</table>

**SP reference architecture comparison**

*Service provider reference architecture for Service Integration Management (SIAM)*

The Service Integration Management Service Integration and Management (SIAM) for service provider (SP) architecture integrates services for a unified customer experience.

**Attributes of SIAM architecture**

- Customers access SP services on a dedicated or shared portal to the SP shared instance.
- SPs use ServiceNow shared instances to manage their service delivery.
SP Reference Architecture – SIAM

- Customer is contracting with best in class service providers for individual services but key operational data needs to be shared across multiple SPs.
- SIAM provides service integration layer for unified customer experience.
- Customer fulfillers operate out of the dedicated instances.

Often de-centralized as each supplier has their own governance programs. However, either a guardian provider or the customer SHOULD force a unified governance committee.

Administration is distributed to each supplier’s own ITSM platform. Integrations/eBonds must be governed for process interactions.

Requesters are generally at the central instance but fulfillers fulfill out of their own supplier instances with the eBonds connecting the flow.

SIAM architecture at a glance
Domain separation terms

With a ServiceNow instance, you can improve efficiency, add greater security, and increase performance for your customer organizations. It’s helpful to understand some of the most common terms as you create your configurations.

Managed domain

In a managed domain, the Managed domain field allows domain administrators to manually select a domain for the user, group, department, location, or CI record, rather than using the domain that is assigned automatically from the company record.

If you want to change those properties, you can override them to further customize the functions of the applications in each of your domains.
Process tables

In process tables, if you see a value in the **Overrides [sys_overrides]** field, a process override record exists. That means that delegated administration, which is how administrators can set domain-specific policies, is in effect. Admins in the global domain can use the **Expand/Collapse Domain Scope** related link to see override records.

When you view process tables from a domain, you see only the relevant process records for the selected domain. When you view a process table from the global domain, the **Expand Domain Scope** related link is displayed to let you see all process records, including overrides. To view only the relevant process records for global again, use the **Collapse Domain Scope** related link.

The domain scope feature is used only for process tables and causes the visibility of data on the table to shift in the opposite direction. For example, a record in the parent domain can be seen in the child, but a parent cannot see a child record. This allows the process to flow down to child domains.
Types of domains

Different types of domains can help you organize your processes and data and how they function in the application or feature.

Customer Domain

In the customer's domain is the user interface, as well as the process that controls how the data is used.

The ACME domain in the following image is a customer domain.

Process Domain

You create processes for how the data is used and what it does in the domain. These processes must have these attributes:

- Specific processes and UI settings for a set of domains
- No core data of any kind (such as specific user data).
• The TOP domain in the following image is a process domain.

**Data Domain**

The data domain holds data that is relevant to multiple customers. That data can be shared without sharing the actual customer domains. Each customer has its own data domain and can access it.

**Note:**

This kind of domain is not common and can cause performance issues if overused. Consult with an SP architect before use.

Example: The domain may hold tasks that ACME, Cisco, and the SP all need to interact with.

The Default domain in the following image is a data domain.

**User Data**

User record data never belongs in the global domain or any of the process domains. Users are primarily created in customer domains and can on occasion be created in data domains.

Admin accounts are special as they should not be used as everyday users of the instance and should be in the global domain to facilitate administrative functions.
Domain hierarchy

Lists, admin, global process

Lists

From the global domain, if you right-click any choice field’s label, select **Configure Choices**, and then add a new choice, the choice pushes automatically to all domain-specific lists for that field. If the new option is marked as **Selected**, it is added as active. If the new option is marked as **Available**, it is added as inactive.

Instance Administration
The instance owner’s administrators must handle all normal process creation, modification, and maintenance in a domain-separated instance. Individual domain managers can maintain some parts of data-driven processes. The types of domain managers maintain user administration, support group memberships, and locations, or manage applications that are designed with tenant administration in mind.

**Global process/parameters**

You can create and maintain the process that affect the global domain as well as set the parameters. These properties are common for all users of a domain-separated instance.

Examples: System properties, dictionary overrides, `sys_documentation` (field labels), the data model (classes, CI types, and so on), tables and fields `[sys_dictionary]` (access can be restricted), indexing (text indexes as well as database), ACLs, installation exits, inbound actions, public pages, and interceptors.

**Creating custom tables in separate domains**

You may need to create custom tables in separate domains because you may want a table to function one way for one customer and another way for another customer.

**Separating a table into domains**

There are four basic sequences to creating separate domains in a table.

1. **Create a `sys_domain` field**

If the Domain Separation plugin hasn't created a separate domain in a table, it's best not to try to force your customization. Use these points as a guideline.

- Create a new field and leave it as a string.
  - Column Name: `sys_domain`
  - Other attributes are defined automatically

  The `sys_domain_path` is created automatically.

The column name `sys_domain` is reserved in the ServiceNow platform, which means that the system recognizes it and automatically applies the appropriate field type and attributes for you. This automatic configuration also creates a corresponding `sys_domain_path` field.

**Note:**

- Set the column name to `sys_domain` rather than using the label.
- Domain separation is not appropriate for every table. If a table is part of the base instance and that table doesn't have a `sys_domain` field, you should leave it that way.

A `sys_domain` field is created automatically when you create a string field with the name “sys_domain.”
2. Add a business rule to set the domain

Your custom tables need business rules to make the table function as it should.

Without business rules
The domain is set to the current domain of the user who creates the record.

With business rules
The domain is not left blank, but is assigned using scripted logic, typically based on the Company field.

The first rule is the **Domain – Set Domain – Task** business rule, which attempts to set the domain of the record based on the record’s company’s domain.

If this rule doesn't find a domain, the **Domain – Default – Task** business rule executes and sets the domain of the record to the default domain.

Then, if the domain of a task record changes, the **Domain – Cascade Domain – Task** business rule changes the domain on all records that are related to the task, such as workflows, metrics, SLAs, and attachments.
3. Add a business rule if Step 2 failed

If the initial business rule fails to set a domain and the domain is still empty or global, a second business rule runs. The second rule examines the `task_for` field that is based on the caller or `requested_for` field. The rule is checking to see if you can set the domain of the record based on the user’s domain. If not, the business rule sets the domain to the default domain. The following image demonstrates these rules.

![Business Rule Table]

- **Name:** Domain – Set Domain  
  **Order:** 100

  **Description:** Business Rule executes before an insert or update on the Task [task] table.

  **Condition:** `current.company.changes() && !current.company.nil()`

  **Script:** `current.sys_domain = current.company.sys_domain;`

- **Name:** Domain – Set Domain - Default  
  **Order:** 9,000

  **Description:** Business Rule executes AFTER Domain – Set Domain – Task.

  **Condition:** `current.sys_domain == 'global' || current.sys_domain.nil()`

  **Script:**

  ```
  /* essentially
   * If (task_for is set)
   * set the domain to the user’s domain
   * ELSE set the domain to the default domain
   */
  ```

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
4. **Add a business rule to cascade the associated records**

Tasks can have many related tables that work together for business objectives. These related records include workflow, SLA, approvals, attachments, and email. If the domain of a task changes, the related records domain must change, too, so they remain visible to the users in the new domain.

This Cascade rule is commonly triggered when you clear records out of the default domain. The following image is an example of a **cascade** business rule.

![Cascade Rule Example](image)

<table>
<thead>
<tr>
<th>Name:</th>
<th>Domain – Cascade Domain - Task</th>
<th>Order:</th>
<th>10,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description:</td>
<td>Business Rule executes AFTER Domain – Set Domain – Default.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Condition:</td>
<td>current.sys_domain.changes()</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Script: | /*
* Keep domains in sync w/related records for:
* workflow context
* workflow executing activities
* workflow history
* task SLAs and related workflows
* approver tables and related workflows
*/ | * group approvals and related workflows
* attachments
* emails
* / |        |

**Customizing domain properties and themes**

You can customize your customers' company properties and themes within the domains that you have configured. Customization makes their instances fit in with their companies' overall look and feel.

**Customizing company themes and logos**

On the company record, you can customize specific design themes and logos for each company.

**Customize the domain**

By default, when you have the service provider plugin installed, the standard business rules contained in the core tables cause the record's domain to be set to the domain of the company that is associated with the record. The company can control the tables such as Task, User, Group, Location, Department, and so on.

With all of these tables, except the Task table, you can override the domain that a record is created in. This gives you more customization options.

**Managing domain separation for specific uses**

You can set up separate domains for email notifications and customize the properties of catalog, tables, users, groups, and views. This enables you to provide more specific behavior in each domain, giving your customers more flexibility.
Emails

You can use separate domains for email notifications and overrides. When you use separate domains for notifications, you can do an override that is based on the domain of just the attached record, not the user’s whole domain.

Service Catalog

The Service Catalog is now domain-separated so that your customers can see and access the catalog. Items are processed as OR conditions when multiple items are used. Service providers should administer the categories and items themselves so they fit their own criteria specifically.

Users and groups

Only use admin accounts in the global domain because admins need access to all domains. Do all your application testing from an actual domain, not in the global domain. Overrides don't process properly in the global domain. Admins should also be given user accounts in production if they are to use the application.

Working with fields

There are several points to consider when you work with fields. Pay close attention to these fields because they can have many variations that affect your configurations.

Lists

There are personal, global, and domain lists, as well as multiple views of each.

Forms

There are global and domain lists as well as multiple views of each.

One database

Any fields that you create exist for all users, in one database. Consider the global impact before you create one.

- ACL scripts cannot keep a field from being viewed in a list because they do not run. You can add a READ ACL to hide a field from users if the ACL is only role-based.

Creating tables

When you create a table, you should add a `sys_domain` or an `sys_overrides` field. Any table that contains data that your instance users need to access, needs the `sys_domain` field. Tables that extend or support processes and that need to flow down to children domains also need the `sys_domain` field.

Configuring domain separation with the domain picker

Use the domain picker wisely, and remember the 80/15/5 approach so that you do not customize too much and impact the performance of your instance.

Verify your domain before making changes

The domain picker gathers all the domains into a list for you to choose from.
If your session times out and even if you don't get logged out, your session falls back to the domain on your user record. You also lose any elevated roles at the same time. In this case, your domain picker could still show the last domain that you selected if the top frame of the list hasn't been reloaded. For this reason, you should reload your list completely if you have been away from the instance for any time.

**Configuring at the TOP domain or the global domain**

Domain separation works best when you are providing services to customers that are mostly standard in their configuration and user and group definition. The more that you customize and create "one-off" solutions, the more you create a margin for error. When you create your processes and business logic, any variations should be in properties that work automatically for each customer. While processes can still be adjusted as needed, use great care when you decide when, and to what degree, to create a unique configuration for a single customer.

You'll need to use an "80-15-5" approach in configuring your domains to avoid too large a margin for customization, and therefore error.

- **Recommended approach for configuration:**
  - 80% or more **Standard**
  - 15% or more **Parametric**
  - Less than 5% **Configuration**

- Determine if a suggested change should be a global or a configurable property.
• Do not overbuild by adding more and more customization that needs to be managed. Instead, do the following:
  • Start with the base system features and verify any gaps before you make any changes.
  • Look for no-code solutions.
  • Use server-side scripts, build modular APIs, and build in domain-separated properties.
  • If you must use client scripting, use only ServiceNow APIs. Limit "synchronous" calls (those that go back and forth from client to server, also called AJAX).
  • Write all scripts logically to keep them simple and effective. Enforce peer reviews of code changes and make sure everyone is following the Domain separation recommended practices for service providers in this section.

Domain separation performance considerations
As you configure domain separation in your application and services, make sure that you consider the number and properties of domains you create. Too many property-heavy domains can impact the performance of your instance.

Limiting property-heavy domains
You can create as many domains as needed, but make sure that you don't create unnecessary domains on the instance. Weighing too many domains on the instance with a lot of properties can impact the performance of your instance.

The number of domains is not what impacts performance but rather what’s in them. Too many properties can slow down the domain picker, which then slows down the overall user experience of your customers. If you are loading the domain picker and already have a large number of domains with a lot of properties, the domain picker has to load all the domains before it gives you control in the session. This process could lead to an outage where you can't access anything on the instance until the domain picker finishes. Before you create new domains, navigate to the domain hierarchy under Domain Admin > Domain Map and make sure that you actually need to create a new domain or whether an existing domain hierarchy can work.

Using the UI16 domain picker
The domain reference picker is available in UI16. With the reference picker, you do not load all the domains at once, but rather the domain is searched as you begin to enter the name of your domain into the domain picker.

Enable the domain reference picker in UI16 by following these steps:
1. In the application navigator, enter sys_properties.list.
2. Set the glide.ui.domain_reference_picker.enabled property to true.
3. Refresh the browser.

Note: Do not upload a large number of domains (over 30) via integration or import sets without doing some testing first or you might bring down your instance.

Setting up domain hierarchies
You can avoid slowdowns and performance impacts in your instance by knowing how domain hierarchies work and by setting them up properly.

Based on the domain hierarchy, users have access to the data in their home domain and any child domains. The process flows down to the child domains and the data rises up.

Make changes to the existing domain hierarchy only when needed. When you update the parent of a domain, the system re-establishes the parent domain with all its child domains that change the domain hierarchy. When the domain hierarchy updates, the system triggers a cascade update on all tables that relate to domains for the records that are created on that domain. As a result, a large number of supporting tables have to be updated too.
For the same reasons, even if you must change the domain hierarchy, never do a mass update. Imagine the number of queries that the system has to run to change the domain hierarchy. Always do an update in small batches. Before you start the next batch of updates, make sure that Domain Work Request (DWR) records are processed. DWRs are reports that display whether there are errors after you’ve changed the domain hierarchy.

**Tracking DWR records**

In the syslog_domain table, look for an information entry for **DWR execution completed.** to confirm that DWR is completed.

---

<table>
<thead>
<tr>
<th>Level</th>
<th>Message</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information</td>
<td>DomainWorkRequestExecutor worker thread pool is shut down. Total time taken for executing the threadpool: 0:00:20</td>
<td>com.glide.domain.par</td>
</tr>
<tr>
<td>Information</td>
<td>DWR execution completed</td>
<td>com.glide.domain.par</td>
</tr>
<tr>
<td>Information</td>
<td>DomainPathUpdater is finished! Total time taken for migration: 0:00:20</td>
<td>com.glide.domain.par</td>
</tr>
<tr>
<td>Information</td>
<td>All DWRs have been processed. Producer will shutdown consumers and exit.</td>
<td>com.glide.domain.par</td>
</tr>
</tbody>
</table>

---

**Domain Work Requests screen**

**Checking domain logs for errors and warnings**

Check the domain logs to find errors or warnings in your domain path processes and hierarchy configurations.

You can find the domain logs in the Domain Log [syslog_domain] table. When the domain hierarchy updates, the system triggers a scheduled job to recalculate the domain paths. The domain logs table captures the results.

Look for any errors and warnings in this table. After reviewing this table, you need to resolve these errors and run the domain path validator again.

In this example of a log, the system has detected ten orphan records in the sys_ui_list table. The errors in these records must be fixed before the domain path can run successfully.
To learn more about domain-separation errors, see Troubleshoot domain separation errors.

**Importance of the Default domain**

Organizing your domains is a crucial part of the domain separation process. If you don't set a default domain, new tasks and user records go to the global domain. Anyone can see the records in the global domain, which means that data can be seen when it isn't supposed to. When you set the default domain, its records are not visible to any user other than an admin.

You should always set one default domain for the domain records on your instance. The default domain is where the system automatically assigns task and user records that are not already assigned to a domain.

When you create a default domain from the Domain Administration screen, add the name Default in the Name field to differentiate it from other domains. Check the Default option as follows:

Maintain regularly the records that you create in the default domain and move them to the correct domains. If records show up often in the default domain, you may need to investigate why. Ideally, you should make sure that all records are created in their appropriate domains (not global or default domains).

**Contains queries and domain access**

Use a "contains" query only in special cases, such as when users or groups need to see data from a domain that they don't have access to, but you don't want to move those users to a domain. Creating domain "contains" and user or group access for a domain should be an exception, only when absolutely needed.

"Contains" is a domain-to-domain relationship that is many-to-many, and has no effect on the flow of process. If you create a large number of domain "contains" relationships or provide broad access, you will generate queries with too
many OR conditions. OR conditions are slow and impact the performance of your instance. Instead of using too many
"contains" relationships, set up your domain hierarchy as follows:

```sql
SELECT ... FROM task task0 ignore index(number) WHERE task0.`sys_class_name` = 'incident' AND (task0.`sys_domain_path` LIKE '%/!' OR task0.`sys_domain_path` LIKE '%/$!/!!/%' OR task0.`sys_domain_path` LIKE '%/$!/!!/$!/!!&/%') ORDER BY task0.`number` DESC limit 0,20
```

**Sample query**

Before you move users to a domain, make sure that they really should have access to that domain. Weigh the benefits
and limitations. The query above is for just one contains relationship. If you have a domain that contains another
domain, and that domain is the parent of a number of other domains, you will have many more OR conditions. Be
careful when you create a domain map so that you do not impact the performance of your instance.

**Domain paths query method**

You can create effective queries with domain paths.

Use domain paths instead of domain spooling (sys_domain) or domain numbering. Queries that use domain paths
are much faster than spooling or numbering.

Domain paths is the default query method for instances that have enabled domain separation.

If you want to verify the query method on your instance, look for the following system properties in the admin
dashboard:

- **If domain path is enabled:** In the System Properties table, you see `glide.sys.domain.provider=domain_paths` and `glide.sys.domain.paths.installed=true`.
- **If domain path is not enabled:** In the System Properties table, you see `glide.sys.domain.provider` != `domain_paths`, `glide.sys.domain.paths.installed=false`.

**Slow queries and SQL debugging**

Debugging SQL and slow queries can help you resolve slowness issues in an instance.

When you debug an instance, you can either enable SQL debugging to look for slow queries or you can look for slow
queries by checking the Slow Queries [sys_query_pattern] table by navigating to System Diagnostics > Stats >
Slow Queries. This table stores all the slow queries in the instance.

When you search the table, look for queries that contain `domain_path` to determine if any slow queries are due to
the domain path in your instance.

If you do find slow queries, try to analyze why they are slow.
Common reasons for slow queries

- A query has too many OR conditions (for more information, see Contains queries and domain access). In the domain hierarchy, place the user or a domain at a hierarchy level where contains or visibility is not
• The query method is not the domain path query method (for more information, see Domain paths query method): If you are not using the domain path query method, contact Customer Service and Support.

• A query needs a database to be indexed so you can see what is in the database quickly. If you can identify the slow query, run the "explain plan" to see if there are options for indexing available. The "explain plan" is a function of SQL that shows the query and what is going on with it.

**Before Query business rules**

You can use a Before Query business rule to help support data segregation on an instance. ServiceNow applications that support domain separation may support the separation of data and data routing only, have advanced business logic separation, or support tenant (customer) level administration of the application.

A Before Query business rule is supplementary code that you use to support data segregation within domain-separated environments.

**Warning:** Do not use the Before Query business rule in place of the Domain Separation plugin. This business rule does not prevent data leakage as securely as the plugin.

**Using the Before Query business rule for data segregation**

You can use the Before Query business rule with data segregation in these situations:

• When domain separation is not supported by a ServiceNow application and you must grant or restrict table or row access to one or more non-internal customers outside of the service provider organization.

**Note:** Before you begin developing, contact ServiceNow Customer Support about the application roadmap for that product; domain support improvements may be planned for upcoming releases.

• When a table is domain-separated but access to its rows must be granted or restricted based on certain conditions that apply only to a set of domains in the system.

  • For example, a customer in the X domain has multiple vendors supporting that domain and those vendors are granted access to see only the records that are assigned to them

**Points to consider before creating Before Query business rules**

You can script Before Query business rules to prevent parent and child table access based on a combination of user information, group memberships, companies, roles, or record-specific field conditions.

• Before Query business rules are put into separate domains and created to apply globally, to a specific branch of a domain hierarchy.

  • Where you can, create Before Query business rules at the lowest possible part of the domain hierarchy so that the rule runs only for users that it applies to.

  • Know that there are scenarios in the system where business rules may not run or where a user-triggered interaction may not trigger a business rule to run. For example, a business rule won't run when you have transform maps with Run business rules turned off, or you have scripts with the workflow disabled.

  • Always populate the condition field to specify when the rule runs. For example, you can specify if the business rule applies only to certain vendors in a domain.

**Warning:** When designing and coding business rules (especially Query business rules), limit OR clauses and searches in non-indexed fields. Too many OR clauses and searches in non-indexed fields can slow queries or affect how your instance performs.
• Use Before Query business rules only when necessary. Too many Before Query rules can affect how your instance performs.

• Before Query business rules run before access control lists (ACLs) and perform better in general. This is true especially when you limit the returned results to those users in service provider (SP) environments who have access to several domains in the system.

• Filtering the data is transparent (unlike with ACLs) to users who do not see the message Data Security restricts... when interacting with data.

When not to use Before Query business rules and ACLs

Be careful when you use Before Query business rules and ACLs to segregate customer data. By using both business rules and ACLs, you create customizations that you then must maintain. Customizations can potentially cause performance issues. Your development teams should create processes to make sure that they don’t break the system.

Domain separation provides both scalability and governance with the current domain path query method (v3), which is a widely supported framework. The ServiceNow Platform and App teams are responsible for maintaining the framework, taking the burden off the customer.

For companies with many customers in many instances, excessive use of Before queries and ACLs may cause the database queries not to perform well.

How domain separation is enabled

You can enable domain separation with a ServiceNow plugin. A product manager, supported by a development team, manages the functionality. Enhancements and fixes for domain separation functionality are included with ServiceNow releases. Instance owners can consult Customer Service and Support resources, such as the Service Portal, at https://support.servicenow.com for assistance with domain separation.

Avoiding domain path in scripts

Domain paths can cause the values of your script to change or even break, so don't use them in scripts.

Your script should not depend on the domain path because if you ever change the domain hierarchy, the domain path recalculates and its value changes. When this happens, your scripts are useless or can throw errors or break. The best strategy is not to write your scripts based on domain paths.

Use the sys_domain field in your scripts rather than depending on the domain path. If you ever change the domain hierarchy, the domain path recalculates and its value changes, which can cause your scripts to be useless, throw errors, or break. Look for base system business rules, which use the sys_domain field, to get some ideas before creating your own scripts.

The ServiceNow platform does not capture the sys_domain_path values in an update set in order to avoid issues with differences in the domain hierarchy for each instance. Therefore, you should validate the domain hierarchy after you import an update set to ensure that the domain path values for your records are correct.

To learn more about domain path, see Request domain separation and Domain Separation Center.
Domain assignments

How you assign a domain impacts the value of the `sys_domain` field. The assignments contain designs and business properties that affect how the application functions in each domain.

Value of the `sys_domain` field

The value of the `sys_domain` field contains the domain that is assigned to the record by any of the following:

- Company to which the user belongs
- Business rule that is used when creating the record
- Module that is used when creating the record
- Form template that is used when creating the record
- Domain of the parent record
- Domain that is assigned to the User record
- Domain of the user who creates it

Make sure that your domain assignment strategies and designs are well documented and tested so that you are creating records as those strategies and designs are inserted into the correct domain. That way you can see that the properties of each domain should you need to duplicate or modify them.

Domain separation and the Customer Service Management (CSM) plugin

For the best outcome, be aware of how the properties in the CSM plugin work. When the plugin is enabled, you can see the status of your records in your domains.

Instance owners should contact Customer Service and Support to enable this property:

- `csm_auto_account_domain_generation`

**Note:** This base system property is located in the system properties table and is available after CSM plugins are enabled.

What the property does

Whenever a new account in the Customer Service application is created, a domain is created and placed under the TOP domain. If the parent field on the account form is populated, and a new record is inserted, it creates that account as a subdomain of the parent.

What happens if this property is not true and the domain is enabled

New account records in a domain-separated environment are automatically placed in the default domain.

In the following image, you can see the status of the records with the plugin enabled.
Domain separation setup and administration

Setting up domain separation involves requesting activation of a plugin, setting options, and assigning users and records to domains.

Do the following to set up domain separation:

1. Request domain separation
2. Create a domain
3. Add a domain field to a table

You can also perform these basic administrative tasks on domains:

- Enable or disable a domain
- View domain relationships
- Expand domain scope
- Create a domain-specific choice list

See Advanced domain separation administration for a list of tasks to perform after you set up domain separation and perform basic administration.

Request domain separation

All domain support features are activated with a plugin called Domain Support - Domain Extensions Installer. Administrators can request activation of this plugin.

To purchase a subscription, contact your ServiceNow account manager. The account manager can arrange to have the plugin activated on your organization's production and sub-production instances, generally within a few days.

If you do not have an account manager, decide to delay activation after purchase, or want to evaluate the product on a sub-production instance without charge, follow these steps.

Role required: admin

If the Domain Support - Domain Extensions Installer plugin is already active, content in the Domain Support - Domain Extensions Installer plugin will not be installed to avoid potential conflict with an existing implementation.

Domain separation replaces Company Separation. Starting with the Helsinki release, the Company Separation plugin can no longer be activated. However, if company separation is already active when you activate domain separation, both plugins are active at the same time. You can control the company separation activation status with the glide.db.separation.field property.
Note: Domain paths are used for all customers on Helsinki and later. Domain numbering is no longer used. Customer Service and Support can assist in the upgrade.

1. Navigate to System Applications > All Available Applications > All.
2. On the All Applications page, click **Request Plugin** to open the Request form on HI.
3. On Now Support, select the redirect link to access the Now Support Service Portal Service Catalog.

<table>
<thead>
<tr>
<th>Activate Plugin</th>
</tr>
</thead>
<tbody>
<tr>
<td>In order to enhance the user experience, we have redesigned Activate a Plugin service catalog. Please use the new HI Service Portal 'Activate a Plugin' service catalog item. You can also use Manage Instances page on Service Portal to Activate a Plugin.</td>
</tr>
<tr>
<td>Take me to the HI Service Portal Activate a Plugin Service Catalog.</td>
</tr>
</tbody>
</table>

4. On the form, fill in the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Instance</td>
<td>Instance on which to activate the plugin.</td>
</tr>
<tr>
<td>Plugin Name</td>
<td>Name of the plugin to activate.</td>
</tr>
<tr>
<td>Specify the date and time you would like this plugin to be enabled</td>
<td>The date and time must be at least two business days from the current time.</td>
</tr>
<tr>
<td>Reason/Comments</td>
<td>Information that would be helpful for the ServiceNow personnel who are activating the plugin. For example, if you need the plugin activated at a specific time instead of during one of the default activation windows, specify that in the comments.</td>
</tr>
</tbody>
</table>

5. Click Submit.

Activating the Domain Extension Installer plugin enables these features:

- Domain separation is based on the Domain [sys_domain] table.
- Delegated administration lets each domain have separate policy.
- All records are part of the global domain.
- The current user's domain determines the domain to use when viewing or operating on a record in a different domain.
Domain separation plugin

The Domain Support - Domain Extensions Installer plugin activates several domain separation features and properties at once. This plugin is typically referred to as the Domain Separation plugin.

Recommended practice for activating the Domain Separation plugin

As part of domain separation development, administrators must request activation of this plugin. For best results, activate the Domain Separation plugin at the start of the development process, preferably before any other plugin is enabled.

If you enable the plugin towards the end of ServiceNow implementation or once an instance has gone live, your application is at risk in both performance and process. On established instances, depending on how things were structured in development, the risk to the platform and its usability could be high. To learn more about domain separation process, see Understanding domain separation.

One risk can happen with the Task table: When the Domain Separation plugin is enabled, the `Domain (sys_domain)` column is added to the table and every existing record is automatically placed in `global`. The instance owner would need to script all these records into the correct domains, which mean there would have to be an established parent/child hierarchy. These types of scripted actions risk data corruption or loss, and possible production down time as large amounts of data would have to be moved. Much of the platform’s code such as business rules, client scripts, form views, workflows, and so on, would be placed into `global` and affected as well.

While that might be acceptable in the ServiceNow base system, if a customer creates code or modifies ServiceNow code, there is risk to platform performance and usability. This is like trying to rewire the main power poles fed into a house while the power is still turned on. Instance owners could severely delay their implementation or experience lengthy down-times in the aftermath of this type of approach.

Features of the Domain Separation plugin

These features are enabled when you activate the plugin:

- Domain separation is based on the Domain `sys_domain` table.
- Delegated administration lets each domain have separate policy.
- All records are part of the global domain.
- The current user's domain determines the domain to use when viewing or operating on a record in a different domain.

Domain system properties and user preferences

Administrators have access to properties and user preferences that control domain scope.

Properties

New activations of domain separation automatically restrict domain scope to the record's domain for all related data or processes. When the user views a record in a form, the record's related data (such as reference picker and related list data) and applied processes (such as business rules and client scripts) are restricted to the record's domain scope. If there are records in multiple tabs, each tab has its own domain scope based on the record opened within that tab. The following properties restrict domain scope to either the record’s domain and the user’s current session domain.
Domain system properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Details</th>
</tr>
</thead>
</table>
| glide.sys.domain.use_record_domain_for_processes | Restricts domain scope to the record's domain for all processes. This property does not apply to business rules. Business rules are always processed from the domain record.                                                                                           * Type: true | false  
  * Default value: true  
  * Location: System Property [sys_properties] table                                                                                                                                                                                                                                           |
| glide.sys.domain.use_record_domain_for_data     | Restricts domain scope to the record's domain for all data.                                                                                                                                                                                                                                                                                                                                                                                                               |
  * Type: true | false  
  * Default value: true in new domain activations from Fuji onwards (upgrades from instances older than Fuji do not have this property in the table)  
  * Location: System Property [sys_properties] table                                                                                                                                                                                                                                           |

When either the **glide.sys.domain.use_record_domain_for_processes** or the **glide.sys.domain.use_record_domain_for_data** property is set to **true**, the following properties are not used, regardless of their setting:

- glide.sys.domain.use_record_domain
- glide.sys.domain.use_record_domain_for_client_scripts
- glide.sys.domain.domain_change_notify
- glide.sys.domain.no_change_roles

For a full list of properties see *Available system properties*.

**Domain scope for business rules executed on the domain table**

In new activations of domain separation starting with the Jakarta release, the session domain determines the business rules executed on the domain table. In previous versions, business rules executed on the domain table were set based on the newly created domain’s hierarchy. This behavior is modified by the **glide.sys.domain.skip_domain_insert_businessrules** property. Setting this property to true significantly improves domain insert performance.

**Domain scope properties for business rules executed on the domain table**

<table>
<thead>
<tr>
<th>Property</th>
<th>Details</th>
</tr>
</thead>
</table>
| glide.sys.domain.skip_domain_insert_businessrules | Specifies the domain scope for business rules executed on the domain table. In new activations of domain separation, the property default is true and business rules are determined by the session domain. In existing implementations, the property default is false and the business rules are determined by the newly created domain’s hierarchy.  
  * Type: true | false  
  * Default value: True in new domain activations starting with Jakarta. False in existing implementations.                                                                                                                                                                                                                                           |
### User preferences

In addition, user administrators can set the following user preference globally or on a per-user basis:

**Domain scope user preferences**

<table>
<thead>
<tr>
<th>Preference</th>
<th>Category</th>
<th>Updated By</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.domain.session_scope</td>
<td>Domain</td>
<td>Admin Only</td>
<td>When true, sets the default scope to the user's session domain rather than the record's domain. When false, the default scope is the record's domain. Users with the domain_expand_scope user role can still change the domain scope as needed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Default value: false</td>
</tr>
<tr>
<td>glide.domain.session_scope_notification</td>
<td></td>
<td>Admin Only</td>
<td>When true, displays a visual cue that record values include an expanded domain scope. When false, the notification is hidden.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Default value: true</td>
</tr>
</tbody>
</table>

### Create a domain

You can create a domain by creating a record in the [domain] table.

Role required: admin

When creating a new domain, keep the following in mind:

- Only one domain can be the default domain.
Only one domain can be the primary domain.

1. Navigate to **Domain Admin > Domains**.
2. Click **New**.
3. Fill in the necessary fields (see table).
4. Click **Submit**.

![Domain Admin new domain form](image)

### Domain form fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique name for the domain.</td>
</tr>
<tr>
<td>Type</td>
<td>Select a domain type that describes the domain. By default the domain types are <strong>Vendor</strong>, <strong>Customer</strong>, and <strong>MSP</strong>. You can also add your own choices.</td>
</tr>
<tr>
<td>Primary</td>
<td>Select the check box if this domain is to be the top-level domain in the hierarchy. The top-level domain only has child domains and no parent domains.</td>
</tr>
<tr>
<td>Default</td>
<td>Select if this domain is to be the default domain for your hierarchy.</td>
</tr>
<tr>
<td>Parent</td>
<td>Select the name of the domain higher in the hierarchy that contains this domain. This field must have a value for the domain to appear in the domain map.</td>
</tr>
<tr>
<td>Active</td>
<td>Select the check box to make the domain available for use. You must select this option for this domain to appear in the domain map.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the domain.</td>
</tr>
</tbody>
</table>

Each domain record can also have several related records:

- Companies
- Contains Domains
- Contained By

To change the domain hierarchy, go to the Contains Domains related list and select the domain records that is the child (contained) domains of the contains relationship.

**Make a domain the default**

The default domain is the domain to which the system automatically assigns task and user records that are not already assigned to a domain.

Role required: admin

1. Navigate to **Domain Admin > Domains**.
2. Open the domain you want to be the default domain. For example, Default.
3. Configure the form layout to add the **Default** field.
4. Select the **Default** check box.
5. Click **Update**.
<table>
<thead>
<tr>
<th>Name</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>WSP 1</td>
</tr>
<tr>
<td>Primary</td>
<td></td>
</tr>
<tr>
<td>Default</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Tasks and users without a domain are placed in this domain when created/updated. This behavior can be overridden by: 1) Unchecking the Default field on this record, or 2) Checking the Default field on another domain record. If no domain is set as Default, tasks and users with no domain are placed in the global domain.</td>
</tr>
</tbody>
</table>

**No records to display**
**Note:** If you do not set a default domain, then new tasks and user records are placed in the global domain.

**Manually manage the domain for particular records**

By default, the system automatically assigns a domain based on the user's company record. In some cases, however, domain administrators want to manually manage which domain a particular record belongs to.

Role required: admin

The **Managed domain** field allows domain administrators to manually select a domain for the user, group, department, location, or CI record, rather than using the domain assigned automatically from the company record. The **Managed domain** field is available on these record types.

- User records
- Group records
- Department records
- Location records
- CI records

1. Navigate to the record you want to manually manage.
2. Select the **Managed** domain check box.
3. From the **Domain** field, select the domain for the record.
4. Click **Update**.

Clearing the **Managed domain** check box hides **Domain** field and the record uses the domain value from the record's company.

**Domain Separated Tables**

You can see at a glance which tables are domain-separated in your instance with the Domain Separated Tables feature.

**Overview**

Use the Domain Separated Tables feature to see which tables are domain-separated. You must activate the **Domain separation plugin** (Domain Support - Domain Extensions Installer), which requires the "maint" role. Start typing "domain" to see the feature appear in the left navigation pane.
You can filter this view to display or remove column names to look for certain properties or attributes that are included in your tables. There are two table types that display on the list:

- Tables that have an explicit `sys_domain` column present, where the Column name displays `sys_domain` value in the list.
- Tables that are using the `domain_master` attribute to derive domain separation from a referenced table, where the Attributes column includes the `domain_master=ref-table` value.

When you use the Show Matching or Filter Out selections on the Column name menu, you can view these two types of tables.
Domain Override Viewer

With the Domain Override Viewer, you can see and manage all your process overrides at once across the entire instance.

Overview

Rather than creating an elaborate search for overrides in your scripts, you can use the Domain Override Viewer to find them quickly.

To launch this feature, begin typing its name in the navigation pane.

The table selector in the Domain Override Viewer displays a list of only the tables that contain record overrides, along with a count of overrides in that table. After you select a table, a list of all parent records with overrides is returned. You can quickly view all parent records, the domain of the parent record, and a count of overrides for each record.

Selecting View Overrides loads a new tab where all overrides, including the parent record, display in the standard list view.
## Domain Override Viewer

Select a table below to display all records with overrides. Select View Overrides on a record to view all of its overrides. Note: Only tables and records with overrides are listed

Please select one table from the dropdown list.

- **Business Rule (sys_script)** - override count: 445
- **Decision (sys_decision_question)** - override count: 1
- **Rule (sysrule)** - override count: 1
- **UI Action (sys_ui_action)** - override count: 10

<table>
<thead>
<tr>
<th>Name</th>
<th>SysID</th>
<th>Domain</th>
<th>Overrides Count</th>
<th>View Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Able to disable parameterized testing</td>
<td>0b6d2974530313008cd9ddee7b12b2</td>
<td>Global</td>
<td>2</td>
<td>View Overrides</td>
</tr>
<tr>
<td>Abort if relationship same scope as list</td>
<td>0468db0693300200d9b9941e867ffbb9e</td>
<td>Global</td>
<td>3</td>
<td>View Overrides</td>
</tr>
<tr>
<td>Abort ratings insert when out of bounds</td>
<td>0f3266ff733023008bcb1c86fbb6a78c</td>
<td>Global</td>
<td>1</td>
<td>View Overrides</td>
</tr>
<tr>
<td>Add Approver If Process Guide running</td>
<td>09a01cc10a0a0b6004eca96095dc87f</td>
<td>Global</td>
<td>2</td>
<td>View Overrides</td>
</tr>
<tr>
<td>Add members to live group</td>
<td>076f62c1d70331002ae9602b6e610311</td>
<td>Global</td>
<td>2</td>
<td>View Overrides</td>
</tr>
<tr>
<td>Add update set id</td>
<td>0edfb33047503200a03a19f9bac9a71f9</td>
<td>Global</td>
<td>1</td>
<td>View Overrides</td>
</tr>
<tr>
<td>Adjust Time Based on Time Zone</td>
<td>0bb491c777d33300b0f5d4082b1061e7</td>
<td>Global</td>
<td>2</td>
<td>View Overrides</td>
</tr>
<tr>
<td>Affected ci notifications</td>
<td>09fa6af10a0a0b1d00c6605ebe45bc26</td>
<td>Global</td>
<td>2</td>
<td>View Overrides</td>
</tr>
<tr>
<td>Affected group notifications</td>
<td>0a6ea4aa0a0b1d006b92f265683131</td>
<td>Global</td>
<td>2</td>
<td>View Overrides</td>
</tr>
</tbody>
</table>
To learn more, see Create domain-separated property overrides.

Enable or disable a domain

When you activate or deactivate a domain, the activation status cascades to companies within the domain.

Role required: admin

When you activate a company record, domain separation automatically activates the company's associated domain. For example, if you activate the ACME company, then you also activate the TOP/ACME domain.

1. Navigate to the domain record.
2. Clear or select the **Active** check box.
3. Click **Update**.

⚠️ **Warning:** Do not delete domains. Deactivate domains that you no longer need instead of deleting them.

Add a domain field to a table

Administrators can domain-separate a custom table by adding a `sys_domain` field to it. However, it is not recommended to add domains to base system tables.

Role required: admin

1. Navigate to the table's list view. For example, type `<table name>.list` in the navigation filter.
2. Right-click the list header and select **Configure > List Layout**.
3. In the **Create new field** section, enter `sys_domain` as the **Name** and **Domain ID** as the **Type**.
4. Click **Add**.
5. Click **Save**.

ℹ️ **Note:** Any other means of creating a field adds a `u_` prefix to the column name. But with the domain field, the system automatically creates the field without the `u_` prefix. You can use the following functionality as a shortcut: Whenever you create a `sys_domain` field, name it `sys_domain` and leave the field type as is. The system automatically sets the field type to **Domain ID** and the field label to **Domain**, saving you a few clicks.

Adding domains to base system tables requires prohibitively thorough testing, updates and adding new logic. In addition in many cases, the source code is not accessible to the customer.

View domain relationships

The domain map offers domain administrators a read-only representation of the active domains on the instance and how they relate to each other.

Role required: admin

All domain maps must have one domain set as the primary domain. In addition, each domain in the domain map must meet these criteria:

- The **Parent** field must be filled in (the primary domain is the only exception to this).
- The **Active** check box must be selected.

The domain map does not draw domain relationships for domains that fail to meet the mapping criteria.

1. Navigate to **Domain Admin > Domain Map**.
2. Click the plus (+) or minus (-) icons on the domain headers to show or hide sub domains.
Select a primary domain
The primary domain indicates the top-level domain in the domain map.

Role required: admin

The primary domain cannot have a parent domain and must have at least one child domain. There can only be one primary domain at a time. If you select another domain as the primary domain, it overrides the previous primary domain.

1. Navigate to Domain Admin > Domains.
2. Select the domain you want to be the primary domain. For example, TOP.
3. Select the Primary check box.
4. Click **Update**.
### Domain

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Primery</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOP</td>
<td>MSP</td>
<td>Yes</td>
<td>Top level, process flows down from here. Overrides from global process are done here.</td>
</tr>
</tbody>
</table>

### Companies

<table>
<thead>
<tr>
<th>Domain = TOP</th>
<th>Name</th>
<th>Street</th>
<th>City</th>
<th>Zip / Postal code</th>
<th>Phone</th>
<th>Updated</th>
</tr>
</thead>
</table>

### Contains Domains

<table>
<thead>
<tr>
<th>Domain = TOP</th>
<th>Contains</th>
</tr>
</thead>
</table>

### Contained By

<table>
<thead>
<tr>
<th>Contains = TOP</th>
<th>Domain</th>
</tr>
</thead>
</table>

Actions on selected rows...
Create Contains relationships between domains
Creating a "contains" relationship between domains changes the domain hierarchy.

Role required: admin

Domains in a contains relationship inherit the settings of the containing domain. The containing domain allows users to see data in the contained domain as well as any of its children. Processes are unaffected by a contains relationship.

1. Navigate to the domain table.
2. Select the domain record that is the parent (container) domain of the new contains relationship.
3. Toggle the domain scope to switch between the session scope and record scope, if necessary.
4. From the Contains Domains related list, click Edit.
5. Select the domain records that is the child (contained) domains of the contains relationship. Only child domains appear by default when the domain picker is set to Global. Toggle the domain scope to see all domains in slushbucket.
6. Click Save, and then click Update.

Expand domain scope
By default, when a user in the global domain views a table containing a sys_overrides column, the user sees records from only the global domain. When an admin in the global domain views a process table, that admin sees only records that are in that process table.

Role required: admin

1. Change the glide.sys.restrict_global_domain_processes property to true.
2. To view records from all domains, click Expand Domain Scope under Related Links.
3. To return to viewing records from the global domain only, click Collapse Domain Scope.

Add domains to a visibility domains list
Adding a visibility domain allows a user or group to see and potentially edit records from another domain regardless of the user or group's normal domain membership.

Role required: admin

Assigning visibility domains to all members of a group is preferred over granting them to individual users.

Note: Adding a visibility domain does not change a table or record's access control rule requirements.

1. Navigate to the group table.
2. Select the group you want to provide with visibility domains.
3. Add the Visibility domains related list to the form.
4. From the Visibility domains related list, click Edit.
5. Select the domain records you want the group or domain to see.
6. Click **Save**, and then click **Update**.

---

**Grant visibility domains to an individual user**

While it is possible to add visibility domains for specific users on the User form, it’s best to add them only via groups. This controls permissions and access should individuals change departments or leave the company.

Role required: **admin**

1. Navigate to **User Administration > User**.
2. Select the user you want to provide with visibility domains.
3. Add the **Visibility domains** related list to the form.
4. From the Visibility Domains related list, click **Edit**.
5. Select the domains whose records you want the user to see.
6. Click **Save**, and then click **Update**.

---

**The Visibility domain embedded list contains the following fields.**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Domain that is visible to the group or user.</td>
</tr>
<tr>
<td>Inherited</td>
<td>Domain is inherited from domain visibility or a parent domain.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Granted By</td>
<td>Name of the group that granted domain visibility.</td>
</tr>
<tr>
<td>Parent visibility</td>
<td>Name of the parent domain and used for grouping records. If the parent record is deleted, then all records with the same parent are deleted as well.</td>
</tr>
</tbody>
</table>

Create a domain-specific choice list

Administrators can configure choice lists to contain entries specific to a particular domain.

Role required: admin

1. Select the domain from domain picker where the choice should be added.
2. Right-click the choice field you want to customize and select **Configure Choices**.
3. Update or add choices.
4. Push changes through the normal change process such as update sets.

**Note:** Administrators should ensure that choices are unique across domains to prevent administrative confusion in the global domain.

If an administrator adds a new choice from the global domain, then users from domains lower in the hierarchy see the new choice at the end of their current choice lists. If the new choice is not active at the global level, then it is available to the domain users via **Configure Choices** but does not show as an active choice.

Advanced domain separation administration

Administrators can view information about domain separation, identify potential issues, and change configuration settings.

You can perform these advanced administrative tasks on domains:

- Use domain selection menus
- View domain relationships

**Use domain selection menus**

The instance offers domain selection via two menu formats.

- Domain selector: provides a simple drop-down list of available domains.
- Domain reference picker: enables a reference field that offers filtering and an auto-complete, type-ahead entry feature. Use this format for longer lists.

The placement of these pickers and the procedure to show or hide them differ depending on the user interface version.

Enable domain selection menus in UI16

Displaying the domain picker in UI16 enables the domain selector by default. After enabling the domain selector, you can add a system property to enable the domain reference picker.

Role required: admin

1. Click the gear icon in the header.
2. On the General tab, click the **Show domain picker in header** switch.

The domain selector appears in the UI16 header.
3. Optional: Enable the domain reference picker.

Note: Enabling the domain reference picker removes the global option from the list. To return to your home domain, click the return arrow next to the reference field. Admin users can click the return arrow to return to the global domain.

a) Enter `sys_properties.list` in the application navigator.
b) If not already present, add the `glide.ui.domain_reference_picker.enabled` property and set the value to `true`.
c) Refresh the browser.

The domain reference picker appears in the UI16 header.

Enable domain selection menus in UI15
Enable the domain selector or the domain reference picker. Use the domain reference picker with auto-complete for long lists that require excessive scrolling.

Role required: admin

On UI15, you must enable a UI macro.

1. Navigate to **System UI > UI Macros**.
2. Select a macro depending on the type of menu you want to enable.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>domain_select</code></td>
<td>Enables the domain selector</td>
</tr>
<tr>
<td><code>domain_reference_picker</code></td>
<td>Enables the domain reference picker</td>
</tr>
</tbody>
</table>

3. Select the **Active** check box, and click **Update**.

Note: If using the domain reference picker, the `domain_select` macro must be set to `false`. If using the domain selector, the `domain_reference_picker` macro must be set to `false`.

4. Refresh the browser.
5. Click the gear icon in the banner frame to show the **Domain** field (UI15).
The domain selector for UI15
Restrict access to the domain picker

Use a system property to restrict access to the domain picker in UI16.

Role required: admin

By default, users with the ITIL role, and roles that include the ITIL role (such as the administrator), can access the domain picker in UI16. You can grant other roles access by adding them to the property or restrict roles by removing them.

2. Add this property: glide.ui.domain_picker.role
3. Configure the property value as a comma-separated list of roles that you want to access the domain picker.

Restrict access to domain selection by role (UI15)

You can include a comma-separated list of roles in domain-related UI macros to restrict access to domain selection by user role.

Role required: admin

This procedure is valid for the pre-UI16 interface. Starting with UI16, you must use a system property to control access to the domain picker. See Restrict access to the domain picker.

1. Navigate to System UI > UI Macros.
2. Select either of the two domain-related UI macros: domain_select or domain_reference_picker.
3. Locate one of the following lines of code:
   - domain_select:
     ```javascript
     var ds = new DomainSelectControl("gsft_domain","itil","Domain","Domain");
     ```
   - domain_reference_picker:
     ```javascript
     var dp = new DomainPicker("${jvar_id}","itil","DomainReference","Domain");
     ```

4. Replace the parameter `itil` with a comma-separated list of roles to control who sees the domain selection menu.

View domain relationships
The domain map offers domain administrators a read-only representation of the active domains on the instance and how they relate to each other.

Role required: admin

All domain maps must have one domain set as the primary domain. In addition, each domain in the domain map must meet these criteria:

- The **Parent** field must be filled in (the primary domain is the only exception to this).
- The **Active** check box must be selected.

The domain map does not draw domain relationships for domains that fail to meet the mapping criteria.

1. Navigate to **Domain Admin > Domain Map**.
2. Click the plus (+) or minus (-) icons on the domain headers to show or hide sub domains.

Domain separation application properties
The Domain Separation plugin has two new tables to give service providers more flexibility in customizing their applications that use domain separation. These tables are the System Application Property table [sys_application_property] and the System Application Property Value table [sys_application_property_value].

New tables offer more options

With service provider (SP) applications, certain actions can vary depending on the domain. However, the ServiceNow® base system System Properties [sys_properties] table is not domain-separated, so it doesn't satisfy the requirements for applications that use domain separation.

Each SP customer may want to customize their applications differently. Previously, features that could be customized were defined as only one global value. Application developers need a more flexible table. Now you can modify your application without having to create code every time you want to add or change the functionality.

How overrides work in the new tables

Developers typically use the ServiceNow System Property [sys_properties] table to create various functions in applications. If you wanted to develop an application to behave differently in different domains, you'd have to customize it yourself.

In the Paris release, the new Application Property [sys_application_property] table simplifies that customization. Instead of going directly to the System Property table for a value, the application property table goes to the System Application table first. This new table now stores the logic that you require to configure your application. If it finds a property in the new table, it uses that content. If there is no information in that table, it moves on to the base system properties table.
When you configure support for domain separation, you can add domain logic to this new Application Properties table. This table can contain properties that don't exist in the System Properties table. Or you can add properties to the configuration table that can override any property that you select in the System Properties table.

For example, let's say that you want to configure an application with a First day of the week feature. Sometimes, you might want the first day of the week to be Sunday. In other cases, you might want the first day of the week to be Monday. In the base system table, there might be only one Day 1 option, which is Sunday. With the new table, you can store another property, making Day 1, Sunday, and a child domain, Monday.

This figure shows how the system draws properties from the Application Property table before going to the System Property [sys_properties]

How scoped apps work in the new table

The new Application Properties table is supported from scoped applications. The application property name, similar to the system property name, is unique, which means that it is prefixed with the scope name if it is not global. The scope of an application impacts your configuration. The scope may determine which Day 1 is defined as Sunday and which as Monday. You can use the same property but customize it so that Day 1, Sunday is the parent domain and
Day 1, Monday is the child domain. In the new table, there is both a domain column and a scope column, so you can set these properties for each.

You can use the Expand Domain Scope view in the `sys_application_property_value` table to show all overrides, as shown in the following image.

![Application Property Values](image)

**Note:**

If those tables are not available, make sure that you have activated the Domain Extension Installer (com.glide.domain.msp_extensions.installer) plugin.

### New application property tables

The new System Application Property `[sys_application_property]` table contains these fields:
• sys_application_property table
  • name
  • description
  • type (choice of string, true|false, integer, time zone, color, and so on)
  • default_value
  • property (ref to sys_properties)
  • usage_notes
  • read_roles
  • write_roles
  • unique key: (name)

The new System Application Property Value [sys_application_property_value] table contains these fields:
• sys_application_property_value table
  • sys_application_property (ref to sys_application_property)
  • sys_domain
  • sys_overrides
  • value
  • unique key: (sys_application_property, sys_domain)

**New APIs**

The new APIs are also supported in scoped apps. Domain-separated application properties have distinct APIs. The GlideApplicationProperty API has two new scriptable methods, available in both global and scoped applications. See GlideApplicationProperty - Scoped, Global to learn more about these new APIs.

**Domain Migration Tool**

Use the Domain Migration Tool to move a customer from a domain-separated environment to their own dedicated instance. After migration, the new instance is not domain separated.

**Domain Migration Tool plugin**

The Domain Migration Tool plugin (com.glide.domain.migration_tool) simplifies the task of moving a customer from a domain-separated environment to a more flexible dedicated instance. Customers may want to migrate to a separate instance to take greater advantage of the Now Platform capabilities.

You must request a cloned instance and request activation of the Domain Migration Tool plugin before you can use it.

The Domain Migration Tool runs only if both data and process separation are enabled in the domain-separated instance:
• The glide.sys.domain.partitioning data property must be set to true.
• The glide.sys.comain.delegated_administration process property must be set to true.

**What the migration tool does**

• Automates much of the migration process, especially cleaning up data
• Migrates the domain-separated instance to a new non-domain-separated instance
• Deletes data from the non-domain-separated instance
**Note:** The tool doesn't delete data that is global, in the target domain, or in additional data domains (if specified).

- Collapses process data, or if unable to collapse deletes process data
- Keeps process records that are visible to the target domain
- Updates the sys_choice, sys_ui_list, and sys_ui_related_list special tables
- Cleans up records added by domain separation plugins:
  - Business rules
  - UI actions
  - Scheduled jobs
  - Installation exits
  - Navigation modules
- Disables domain separation and removes domains from the cloned instance:
  - Sets these properties to `false` in the cloned instance:
    - `glide.sys.domain.partitioning`
    - `glide.sys.domain.delegated_administration`
    - `glide.sys.domain.enabled`
  - Deletes all domains except the target domain and any additional specified data domains
- Updates the `Status` field in the domain_migration_tool_status table
  
The `Status` is `Finished` when the tool completes the process.
- Logs progress and status to syslog_domain
  
The source is `MigrationTool` for all log entries associated with migration.
  - Logs each data table and how many data tables remain
  - Logs each process table and which domain’s records are currently being inactivated or deleted

### What the migration tool doesn't do

- Clone the instance
  
  You must request Support to clone the instance for you before you can use the tool.
- Create another domain-separated instance
- Manage data in the source domain-separated instance
- Migrate records (data or process) if either data or process separation properties are disabled before you run the tool
- Alter any data on the source instance
- Delete data that is global, in the target domain, or in additional data domains (if specified)

### What you must do after running the tool

The Domain Migration Tool automates the removal of data outside the desired domains (the target domain, any additional data domains, and the global domain). You must evaluate all the remaining configurations to ensure that they are appropriate and work for your non-domain-separated instance. For example, if you had a business rule that set the domain field on records, you might want to disable this business rule, since it no longer serves a purpose.
Migrate a domain-separated instance to a dedicated instance
Move a customer from a domain-separated environment into their own dedicated instance environment.

Role required: admin

1. Navigate to **domain_migration_tool_status.list**.
2. Click **New**.
3. Complete the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target domain</td>
<td>Specify the domain you want to migrate. This is the domain used for both process and data. Only the target domain is retained, not any of its children, unless specified in the <strong>Additional data domains</strong> field.</td>
</tr>
<tr>
<td>Additional data domains</td>
<td>Optionally, specify any additional data domains you want to migrate. If you want to migrate the target domain and all of its children, you must specify all children.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.
5. Open the form you just submitted.
6. Click **Start Migration**.
7. The **Status** is updated as the tool performs its functions.
   The **Status** is **Finished** when the migration is complete.

**Process administration**

Process administration allows administrators to set domain-specific policies.

The policies set lower in the domain hierarchy override policies set higher in the domain hierarchy. While in a domain, administrators can set domain-specific versions of these global policies and settings:

- Client scripts
- System policies
- Application and module names
- Application roles
- Module filters

**Warning:** All users with the admin role have special access to all system features, functions, and data because administrators can override ACL rules and pass all role checks. Grant this privilege carefully.

When users have the **admin** role, then all policies in the instance are available to them regardless of the assigned domain. They can enter a specific domain, and then only policies in that domain or higher are visible and processed during a relevant transaction. When an administrator modifies a policy that is in a higher domain or the global domain, the system automatically creates a new record for that administrator's current domain. It does not modify the original policy, application, or module record. This new record overrides the original.

To make changes to a policy in a lower-level domain, go into that domain and modify the policy. This approach creates the new policy record in your domain that overrides the original, higher-level policy record.

Do not make changes on the higher-level policy and then change the **Domain** field on that policy. This approach does not create a policy record in your lower-level domain, nor does it keep the policy record for the higher-level domain.
The `sys_overrides` field indicates that a policy, application, or module at a lower level in the hierarchy overrides a record at a higher level. The system automatically sets this field when an administrator attempts to modify a policy, application, or module that belongs to another domain higher in the hierarchy. Again, rather than actually changing the higher level record, the attempted update is changed into an insert, and the `sys_overrides` field is set to indicate the higher level policy, application, or module that is being overridden. Later when the records for a relevant transaction are loaded, the overriding domain-specific policy, application, or module is used instead of the original.

**Domains for process administration**

By default, process administration always uses the record's domain to determine what policies to apply.

The record's domain takes precedence over the user's domain. If there are no policies in the record's domain, delegated administration checks for policies in the next highest level of the domain hierarchy. The search for domain policies continues up the domain hierarchy until reaching the global domain. If there are no domain policies lower in the domain hierarchy, processes administration uses the policies for the global domain.

For example, Fred Luddy is a user in the Acme domain who can see records in the child domains of Acme: Atlanta, Acme: San Diego, and Acme: NY child domains. When he opens a record in the Acme: San Diego domain, process administration first checks for policies in the Acme: San Diego domain. If there are no policies at this level of the domain hierarchy, process administration checks for policies from the Acme domain. If there are no policies in the Acme domain, process administration uses the global domain policies as there are no other domains higher in the domain hierarchy.

**Sample process administration with domain specific applications**

The following example illustrates process administration with domain-specific applications and modules.

As the administrator of the Oceanic domain, David Loo decides to customize the Configuration application. To start with, David reviews the modules available in the Configuration application module.
Starting view of the Configuration application

David decides to rename the Configuration application to CMDB and to allow the inventory_admin role to see the application.
### Sample domain-specific changes to the Configuration application

<table>
<thead>
<tr>
<th>Title</th>
<th>Active</th>
<th>Order</th>
<th>Roles</th>
<th>Name</th>
<th>Domain</th>
<th>Overrides</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Management</td>
<td>true</td>
<td>900</td>
<td>admin</td>
<td>asset</td>
<td>global</td>
<td></td>
</tr>
<tr>
<td>BSM Map</td>
<td>true</td>
<td></td>
<td>admin</td>
<td>bsm_map</td>
<td>global</td>
<td></td>
</tr>
<tr>
<td>Change</td>
<td>true</td>
<td>400</td>
<td>iti</td>
<td>change_management</td>
<td>global</td>
<td></td>
</tr>
<tr>
<td>CMDB</td>
<td>true</td>
<td>600</td>
<td>inventory_admin</td>
<td>configuration_management</td>
<td></td>
<td>Database configuration_management</td>
</tr>
<tr>
<td>Content Management</td>
<td>true</td>
<td></td>
<td>content_admin</td>
<td>cms</td>
<td>global</td>
<td></td>
</tr>
<tr>
<td>Contract Management</td>
<td>true</td>
<td>1,000</td>
<td>asset</td>
<td>asset_contracts</td>
<td>global</td>
<td></td>
</tr>
<tr>
<td>ECC</td>
<td>true</td>
<td></td>
<td>admin</td>
<td>ecc</td>
<td>global</td>
<td></td>
</tr>
<tr>
<td>Homepege Admin</td>
<td>true</td>
<td></td>
<td>admin</td>
<td>home</td>
<td>global</td>
<td></td>
</tr>
<tr>
<td>Incident</td>
<td>true</td>
<td>200</td>
<td>iti</td>
<td>incident_management</td>
<td>global</td>
<td></td>
</tr>
<tr>
<td>Instance Clone</td>
<td>true</td>
<td></td>
<td>clone_admin</td>
<td>instance_clone</td>
<td>global</td>
<td></td>
</tr>
<tr>
<td>Knowledge Base</td>
<td>true</td>
<td>800</td>
<td>iti_admin</td>
<td>knowledge</td>
<td>global</td>
<td></td>
</tr>
<tr>
<td>Metrics</td>
<td>true</td>
<td></td>
<td>iti_admin</td>
<td>metrics</td>
<td>global</td>
<td></td>
</tr>
<tr>
<td>MID Server</td>
<td>true</td>
<td></td>
<td>admin</td>
<td>MID</td>
<td>global</td>
<td></td>
</tr>
<tr>
<td>Organization Management</td>
<td>true</td>
<td>875</td>
<td>asset</td>
<td>organization_management</td>
<td>global</td>
<td></td>
</tr>
<tr>
<td>Problem</td>
<td>true</td>
<td>300</td>
<td>iti</td>
<td>problem_management</td>
<td>global</td>
<td></td>
</tr>
<tr>
<td>Reports</td>
<td>true</td>
<td>1,100</td>
<td>iti</td>
<td>reports</td>
<td>global</td>
<td></td>
</tr>
<tr>
<td>SAML 2 Single Sign-on</td>
<td>true</td>
<td></td>
<td>admin</td>
<td>saml_2_single_sign_on</td>
<td>global</td>
<td></td>
</tr>
<tr>
<td>SAML Single Sign-on</td>
<td>true</td>
<td></td>
<td>admin</td>
<td>SAML_Single_Sign-on</td>
<td>global</td>
<td></td>
</tr>
</tbody>
</table>

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
Next, David decides to change the Incident application by activating the **Open - in "New" State** module and adding a new filter item to show open incidents in the Oceanic category.

**Sample domain-specific changes to the Open - "New" State module**

This creates a new module entry in the application rather than overwriting the existing module in the global domain.
### Application - Incident Management

<table>
<thead>
<tr>
<th>Title</th>
<th>Table</th>
<th>Active</th>
<th>Filter</th>
<th>Order</th>
<th>Link Type</th>
<th>Roles</th>
<th>Domain</th>
<th>Overrides</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create New</td>
<td>incident</td>
<td>true</td>
<td></td>
<td>100</td>
<td>URL (from Arguments)</td>
<td></td>
<td>global</td>
<td></td>
</tr>
<tr>
<td>Assigned to me</td>
<td>incident</td>
<td>true</td>
<td>active=true<em>assigned_to</em>javascript:my...</td>
<td>150</td>
<td>List of Records</td>
<td></td>
<td>global</td>
<td></td>
</tr>
<tr>
<td>Open</td>
<td>incident</td>
<td>true</td>
<td>active=true*EQ</td>
<td>200</td>
<td>List of Records</td>
<td></td>
<td>global</td>
<td></td>
</tr>
<tr>
<td>Open in &quot;New&quot; state</td>
<td>incident</td>
<td>true</td>
<td>incident_state=1<em>active=true</em>category=da...</td>
<td>200</td>
<td>List of Records</td>
<td></td>
<td>global</td>
<td></td>
</tr>
<tr>
<td>Open - Unassigned</td>
<td>incident</td>
<td>true</td>
<td>assigned_to=NULL<em>active=true</em>EQ</td>
<td>300</td>
<td>List of Records</td>
<td></td>
<td>global</td>
<td></td>
</tr>
<tr>
<td>Received</td>
<td>incident</td>
<td>true</td>
<td>status=8*EQ</td>
<td>325</td>
<td>List of Records</td>
<td></td>
<td>global</td>
<td></td>
</tr>
<tr>
<td>Closed</td>
<td>incident</td>
<td>true</td>
<td>active=false*EQ</td>
<td>350</td>
<td>List of Records</td>
<td></td>
<td>global</td>
<td></td>
</tr>
<tr>
<td>All</td>
<td>incident</td>
<td>true</td>
<td></td>
<td>400</td>
<td>URL (from Arguments)</td>
<td></td>
<td>global</td>
<td></td>
</tr>
<tr>
<td>Overview</td>
<td>true</td>
<td></td>
<td></td>
<td>500</td>
<td>URL (from Arguments)</td>
<td></td>
<td>global</td>
<td></td>
</tr>
<tr>
<td>Critical Incidents Map</td>
<td>incident true</td>
<td></td>
<td>600</td>
<td>URL (from Arguments)</td>
<td></td>
<td>global</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trend Chart</td>
<td>sys_dashboard_template</td>
<td>false</td>
<td></td>
<td>700</td>
<td>URL (from Arguments)</td>
<td></td>
<td>global</td>
<td></td>
</tr>
</tbody>
</table>
If another administrator from another domain, such as Fred Luddy, logs in and looks at the Configuration application, the settings from the global domain appear.

David Loo’s view of applications
Enable verbose domain logging and debug messages

Domain log and debug messages allow you to troubleshoot domain configuration errors.

Role required: admin

1. In the Domain Separation Center, navigate to Domain Admin.
2. Click Configure Domain Center.
3. For Enable verbose domain logging, select the Yes check box.
4. Click Update.

View a real-time domain message

You can view real-time domain messages from the system logs.

Role required: admin

1. Enable verbose domain logging: Navigate to Domain Admin > Domain Separation Center > Configure Domain Center > Enables detail domain logging > Yes (or set property glide.sys.domain.verbose to True).
2. Navigate to System Diagnostics > Session Debug > Enable All. Because this is a real time review, there is no need to let the debug session run for a time before checking the log files.
4. Search for the text Query against table.

This query finds log messages in this format:

```
08:36:43.974: [Domain Paths] Query against table incident restricted by domain values [Database Atlanta[db53580b0a0a0a6501aa37c294a2ba6b], Database[287ee6fea9fe198100ada7950d0b1b73],
```
In this example, the user viewing the Incident table only saw records that matched the Database Atlanta, Database, Database San Diego, global, and NY DB domains.

**View a historical domain message**

You can view historical domain messages in the log file to troubleshoot domain separation issues.

Role required: admin

1. Enable verbose domain logging: Navigate to **Domain Admin > Domain Separation Center > Configure Domain Center > Enables detail domain logging > Yes** (or set property `glide.sys.domain.verbose` to `True`).
2. Navigate to **System Diagnostics > Session Debug > Enable All**.
3. Let the debug session run for a time period, such as a day, before checking the log files.
4. Navigate to **System Logs > Utilities > Node Log File Download**.
5. Open the record for the day you want to view. Log files use the naming format `localhost_log.<yyyy-mm-dd>.txt`.
6. Click the **Download** log related link.
7. Open the downloaded log file in a text editor and search for log messages with the following format:

   ```json
   Query against table incident restricted by domain values [global, Software[8a4dde73c6112278017a6a4baf547aa7]]
   ```

   In this example, a user only saw records from the Incident table that matched the global and Software domains.

**Troubleshoot domain separation errors**

If you encounter domain separation issues, review this list of solutions.

<table>
<thead>
<tr>
<th>Error or symptom</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>A domain sys_id points to a non-existent domain</td>
<td>This error occurs when a data record, such as a user or task record, has a <code>sys_domain</code> column value whose <code>sys_id</code> does not exist in the current domain table. The domain <code>sys_id</code> could have been accidentally deleted or it could refer to a previous domain table if you changed the domain table. To fix the error, open a list for the table containing the error, filter on the invalid <code>sys_domain</code> value. Then, either manually enter the correct <code>sys_domain</code> value or remove it.</td>
</tr>
</tbody>
</table>

**Note:** You can have invalid domain `sys_ids` in any table that references the domain table. For example, invalid domain IDs can occur in the User Visibility Domain `[sys_user_visibility]`, Group Visibility Domain `[sys_user_group_visibility]`, and Contained Domain `[domain_contains]` tables.

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
<table>
<thead>
<tr>
<th>Error or symptom</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>A domain path or domain number sys_id points to the wrong domain</td>
<td>This error occurs when a domain number or domain path query is out of sync with the actual domain name. This error can occur with domain numbers when adding domains requires renumbering or during the conversion from domain numbers to domain paths. To fix the error, check the results in the Domain Separation Center. If the error persists, you can manually edit the value for the <code>sys_domain_path</code> or <code>sys_domain_number</code> columns to point to the proper domain.</td>
</tr>
<tr>
<td>The domain tree structure is corrupt</td>
<td>This error occurs if there is a series of domain contains relationships that create an infinite loop among domains. To fix the error, open a list for the domain table and manually edit the domain contains values to not form a loop.</td>
</tr>
</tbody>
</table>

**Domain Separation Center**

Audit your domains regularly to reveal problems.

**What is the Domain Separation Center?**

The Domain Separation Center is a dashboard where you can schedule and configure audits for all of the domains stored in your domain_audit_definition table. The dashboard enables you to review audit results and dig deeper into domain errors and warnings. You can find the Domain Separation Center dashboard at `<ServiceNow-instance-name>/domaincenter`.

The Domain Separation Center provides many audits. You cannot create your own. You can, however, configure how often they run. Audits run on all of the domains stored in the domain_audit_definition table.
Configure audits

You can configure whether an audit is active and how frequently it runs.

1. In the Domain Separation Center, click **Configure Audits**.

   The **Configure Audits** page displays.
2. Configure each audit you want to be active. Audits are inactive by default.
   a. Click an audit.
   b. Click the Active box to activate the audit.
   c. Specify how often the audit runs in the Frequency field.
      The Domain Separation Center runs all audits marked with the same frequency at the same time. Do not select Daily for audits run on large tables.
   d. Repeat these steps for each audit you want to activate.

3. Click Save.

Schedule audits

You configured one or more audits to run daily, weekly, or monthly. The scheduler specifies what days and times to run those audits. All audits with the same scheduling frequency run sequentially staring at the time you configure.

1. In the Domain Separation Center, click Audit Schedules.
   The Audit Schedule page displays.
2. Configure the audit schedules.
   a. Click a schedule name.
   b. Specify the time of day to run the audit.
      Time units are 24 hour clocks, that is, 14 equals 2 PM.
   c. For weekly schedules, select the day of the week to run the audit, where 1 is Sunday.
   d. For monthly schedules, select the day of the month to run the audit.
   e. Repeat the procedure for the other schedules.
3. Click Save to save the configuration changes.
4. Click Execute Now to run all of the audits scheduled to run at the frequency shown at the top of the right pane, for example, if the pane title is, Domain Audit Schedule - Daily, all of the audits that run daily are run.

To see the status of a running audit, in the Domain Separation Center, click the number in the Running Audits box.

Execute audits immediately

Audits typically run as scheduled. You can, however run all audits on command.

1. In the Domain Separation Center, click Audit Schedules.
   The Audit Schedule page displays.
2. Click the name of the audit schedule you want to run, for example, daily, weekly, or monthly.
3. Click Execute Now.

To see the status of a running audit, in the Domain Separation Center, click the number in the Running Audits box.
Configure the Domain Separation Center

1. In the Domain Separation Center, click **Configure Domain Center**.

2. On the **Configure Domain Center** page, for **Enables detail domain logging**, select **Yes** to store detailed logs that help diagnose domain-related issues. Detailed logging might cause performance issues. These logs refer to server-side logs in the syslog_domain table. For information about viewing the logs, see View audits with warnings and failures.

3. In the slushbucket, move into the **Selected** column all of your large tables.

   Daily audits should not run on large tables. Grayed-out table names in the **Selected** column are large and cannot be moved to the **Available** column.

4. Click **Update**.

View audits with warnings and failures

On the dashboard, **Errors** and **Warnings** provide detailed information about audits that encountered problems. Logs related to domain separation reside on your server in the syslog_domain table.

1. In the Domain Separation Center, click the number in the **Errors** or **Warnings** box.

   The **Errors** or **Warnings** page displays, respectively.

2. Click one of the audits in the list.

   The page displays detailed information about problems with the audit you selected. The messages in **Audit Result Details** refer to values in the syslog_domain table for table audits that revealed errors or warnings.

3. To see the logs on the server that provide information about warning or error audits:

   a. Copy the **Detail ID** value in the left panel of a warning or error.
   
   b. In the Filter Navigator of HI, enter **syslog_domain.do**.

      The Domain Log page displays.

   c. In the **Source** search field, enter `=<Detail-ID>` (no space after the equals sign), for example, `=f6a00fd29a85b30a9503a81b9169678`.

      The Domain Log page displays only the logs related to the audit with the Detail ID you specified. Each row in the table specifies a different record the audit found problems in. Notice that the **Message** field on this page matches the values displayed in the Domain Service Center's **Message** column. The format of the message matches the audit type.

4. Click:

   - **Rerun Audit**—Rerun an audit to see if it still encounters a warning or error.
   - **Deactivate Audit**—Inactivate an audit.
   - **Copy Details**—Copy audit details to the clipboard.

View running and pending audits

Active audits periodically run or are queued to run, as scheduled. You can view their status as they run.
1. Click the number in the **Running Audits** box to view audits that are currently running or pending running.
   
   The **Running Audits** page displays.

2. Click an audit for more information about it.

### View inactive audits

1. Click the number in the **Inactive Audits** box.
   
   The **Inactive Audits** page displays all of the audits that are currently deactivated.

2. Click one of the audits to display more information about it.

3. To activate an audit, click the **Active** box and use the **Frequency** field to specify how often the audit runs.

4. Click **Update**.

### Configure the Domain Separation Center

Specify which tables in domains are large and whether you want detailed logging.

Role required: admin

You can schedule audits to run on a daily, weekly, or monthly basis. Audits run on very large tables can take a significant amount of time. For that reason, we advise you not to run audits daily on large tables. Starting a new audit on one that is taking more than a day to run can have negative consequences.

Detailed logging can provide greater insights into problems found during audits. Detailed logging, however, may hurt performance.

1. In the Domain Separation Center, click **Configure Domain Center**.
   
   The Configure Domain Center page appears.

2. For **Enables detail domain logging**, select **Yes** to store detailed logs that help diagnose domain-related issues. Detailed logging might cause performance issues.
   
   These logs refer to server-side logs in the syslog_domain table. For information about viewing the logs, see the **View audits with warnings and failures** section below.

3. In the slushbucket, move all of your large tables into the **Selected** column.
   
   Daily audits should not run on large tables. Grayed-out table names in the **Selected** column are large and cannot be moved to the **Available** column.

4. Click **Update**.

5. If you have very large tables that should never be audited, set the **com.glide.domain.audit.big_tables.additional** system property to a comma-separated list of those table names.

### Configure audits

You can configure whether an audit is active and how frequently it runs.

Role required: admin

1. In the Domain Separation Center, click **Configure Audits**.
   
   The Configure Audits page appears.

2. Configure each audit you want to be active. Audits are inactive by default.
   
   a) Click an audit.

   b) Click the **Active** check box to activate the audit.
c) Specify how often the audit runs in the **Frequency** field.

The Domain Separation Center runs all audits marked with the same frequency at the same time. Do not select **Daily** for audits run on large tables.

d) Repeat steps a-c for each audit you want to activate.

3. Click **Save**.

**Schedule audits**

Specify the time and day that audits are run.

Role required: admin

You configured one or more audits to run daily, weekly, or monthly. The scheduler specifies what days and times to run those audits. All audits with the same scheduling frequency run sequentially starting at the time you configure.

1. In the Domain Separation Center, click **Audit Schedules**.

   The Audit Schedule page appears.

2. Configure the audit schedules.

   a) Click a schedule name.

   b) Specify the time of day to run the audit.

   Time units use the 24-hour clock (that is, 14 equals 2 PM).

   c) For weekly schedules, select the day of the week to run the audit, where 1 is Sunday.

   d) For monthly schedules, select the day of the month to run the audit.

   e) Repeat the procedure for the other schedules.

3. Click **Save** to save the configuration changes.

4. Optional: Click **Execute Now** to run all the audits scheduled to run at the frequency shown at the top of the right pane.

   For example, if the pane title is **Domain Audit Schedule - Daily**, **Execute Now** immediately runs all the audits that are scheduled to run daily.

To see the status of a running audit, in the Domain Separation Center, click the number in the **Running Audits** box.

**Execute audits immediately**

Audits typically run as scheduled. You can, however, run all audits on command.

Role required: admin

You cannot run individual audits manually. You can, however, run all audits that are configured with the same scheduling frequency. For example, you can run all audits that are configured to run daily.

1. In the Domain Separation Center, click **Audit Schedules**.

2. Click the name of the audit schedule you want to run (for example, daily, weekly, or monthly).

3. Click **Execute Now**.

To see the status of a running audit, in the Domain Separation Center, click the number in the **Running Audits** box.

**View audits with warnings and errors**

The Domain Separation Center provides details about audit errors and warnings.

Role required: admin
On the Service Domain Center dashboard, **Errors** and **Warnings** provide detailed information about audits that encountered problems. Logs related to domain separation reside on your server in the syslog_domain table. Errors are issues that require immediate attention. Warnings do not lead to failures but present best practices, for example, not making the domain name too long.

1. In the Domain Separation Center, click the number in the **Errors** or **Warnings** box. The **Errors** or **Warnings** page appears.
2. Click one of the audits in the list. The page displays detailed information about problems with the audit you selected. The messages in **Audit Result Details** refer to values in the syslog_domain table on the server for table audits that revealed errors or warnings.
3. To see the logs on the server that provide information about warning or error audits:
   a) Copy the **Detail ID** value in the left panel of a warning or error.
   b) On the instance running the Domain Separation Center, in the **Filter navigator**, enter `syslog_domain.list`. The Domain Log page appears.
   c) In the search field of the **Source** column, enter `=<Detail-ID>` (no space after the equals sign), for example, `=f6a00fd29a85b300a9503a81b9169678`. The Domain Log page displays only the logs related to the audit with the Detail ID you specified. Each row in the table specifies a different record the audit found problems in. Notice that the **Message** field on this page matches the values displayed in the **Message** column of the Domain Service Center. The information included in the message matches the audit type.

4. Optionally, click:
   - **Rerun Audit** — Rerun an audit to see if it still encounters a warning or error.
   - **Deactivate Audit** — Inactivate an audit.
   - **Copy Details** — Copy audit details to the clipboard.

### View running and pending results

You can view running and pending audits to see their status.

Role required: admin

Active audits periodically run or are queued to run, as scheduled. You can view their status as they run.

1. Click the number in the **Running Audits** box to view audits that are currently running or pending running. The Running Audits page appears.
2. Click a running or pending audit to see information about it.

### View inactive audits

You can view all inactive audits in one place and optionally activate them.

Role required: admin

1. Click the number in the **Inactive Audits** box. The Inactive Audits page displays all the audits that are currently deactivated.
2. Click one of the audits to display more information about it.
3. Optional: Activate an audit by clicking the **Active** box and specifying how often the audit runs in the **Frequency** field.
4. Click **Update**.
Upgrades and conversions

The ServiceNow platform includes tools to help you during and after an upgrade, and also allows you to convert a ServiceNow Express instance to a ServiceNow Service Management enterprise platform.

See also

Upgrade to .

The upgrade process moves your instance to a new ServiceNow release version. Understand the difference between upgrading and patching, release definitions, rollback and backup options, and how to test your non-production and production instance upgrades.

Upgrade History module: Track every upgrade

The Upgrade History module tracks every upgrade made to an instance. Administrators can use the module to resolve upgrade conflicts and optionally to revert customizations to base system versions to take advantage of new features.

An upgrade history record is created for each upgrade that is run. To view an upgrade history record, navigate to System Diagnostics > Upgrade History and click the upgrade.

Note: Debug Upgrade provides detailed debugging output for transactions containing artifacts affected by the most recent upgrade, and is designed to assist in upgrade error resolution. See Debug upgrade.

Note: The Payload and Payload Hash fields have been removed from the Upgrade History record in a previous release.

Upgrade History record

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From</td>
<td>Name of the previous .war file (version).</td>
</tr>
<tr>
<td>To</td>
<td>Name of the applied .war file (version).</td>
</tr>
<tr>
<td>Upgrade started</td>
<td>Time stamp when the upgrade process began.</td>
</tr>
<tr>
<td>Upgrade finished</td>
<td>Time stamp when the upgrade process was completed.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Changes skipped</td>
<td>Total number of records that were different from the previous upgrade but were skipped, mostly likely due to customization. Changes skipped is the sum of the records that have disposition of skipped manual merge (where the value of changed is true), added to the number of records that have disposition of skipped error, added to the number of records that were skipped and different.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> To prevent your customizations from being overwritten during system upgrades, the upgrade process skips (does not apply the update to) objects that have been customized. One of your responsibilities as the administrator is to resolve each update that was skipped due to a customization. To resolve a skipped update, you review the reason for each skipped record and then either merge the customization or revert the customization to the base system.</td>
</tr>
<tr>
<td>Changes applied</td>
<td>Total number of the changes that were applied in this upgrade. Changes applied is sum of updated and different records, added to the number of deleted records (where the value of changed is true) added to the number of inserted records (where the value of changed is true).</td>
</tr>
<tr>
<td>Changes processed</td>
<td>Total number of items processed during this upgrade. Changes processed is the sum of Changes skipped, plus Changes applied.</td>
</tr>
</tbody>
</table>

### Upgrade History Details form section

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updated and different</td>
<td>Number of Upgrade Detail records for which the value of the disposition is updated, and the value of changed is equal to true. This does not appear on the form by default.</td>
</tr>
<tr>
<td>Updated and not different</td>
<td>Number of Upgrade Detail records for which the value of the disposition is updated, and the value of changed is equal to false. This does not appear on the form by default.</td>
</tr>
<tr>
<td>Skipped and different</td>
<td>Number of Upgrade Detail records for which the value of the disposition is skipped, and the value of changed is equal to true. This does not appear on the form by default.</td>
</tr>
<tr>
<td>Skipped and not different</td>
<td>Number of Upgrade Detail records for which the value of the disposition is skipped, and the value of changed is equal to false. This does not appear on the form by default.</td>
</tr>
</tbody>
</table>
**Review Skipped Records form section**

The Skipped Changes to Review related list displays each record that was skipped during the upgrade process. Use the list to review the reason for each skipped record in the list and then either merge your customization or revert your customization to the base system.

**Skipped Changes to Review related list**

To prevent your customizations from being overwritten during system upgrades, the upgrade process skips (does not apply the update to) objects that have been customized. To assist you in tracking and resolving skipped update records that need review, Skipped Changes to Review lists all updates skipped during the upgrade process.

By default, the list is filtered by Disposition Skipped Error, Disposition Skipped Manual Merge, Disposition Skipped, or Disposition Skipped (second pass), and the resolution status is either empty or not reviewed.

Navigate to **System Diagnostics > Upgrade History** to view the Skipped Changes to Review related list.

<table>
<thead>
<tr>
<th>Field</th>
<th>Input Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>File name</td>
<td>Name of skipped Upgrade Detail record.</td>
</tr>
<tr>
<td>Disposition</td>
<td>Action performed on this file during the selected upgrade:</td>
</tr>
<tr>
<td></td>
<td>• Inserted: The system inserted a new record.</td>
</tr>
<tr>
<td></td>
<td>• Updated: The system updated this record.</td>
</tr>
<tr>
<td></td>
<td>• Deleted: The system deleted this record.</td>
</tr>
<tr>
<td></td>
<td>• Skipped: The system did not change this record in order to preserve</td>
</tr>
<tr>
<td></td>
<td>customizations.</td>
</tr>
<tr>
<td></td>
<td>• Reverted: This record was reverted to the base version.</td>
</tr>
<tr>
<td></td>
<td>• Table not found: The system could not find the table containing this</td>
</tr>
<tr>
<td></td>
<td>record.</td>
</tr>
<tr>
<td></td>
<td>• Unchanged: The system did not change this record because the baseline</td>
</tr>
<tr>
<td></td>
<td>component has not changed since the last release.</td>
</tr>
<tr>
<td></td>
<td>• Skipped Manual Merge: The system did not change this record because</td>
</tr>
<tr>
<td></td>
<td>updating it requires manual intervention.</td>
</tr>
<tr>
<td></td>
<td>• Skipped Apply Once: The system skipped this record because it had</td>
</tr>
<tr>
<td></td>
<td>already applied an update from an xml file in the apply once folder.</td>
</tr>
<tr>
<td></td>
<td>• Not Latest: The system applied a change, but this change was</td>
</tr>
<tr>
<td></td>
<td>overwritten later during the same upgrade.</td>
</tr>
</tbody>
</table>
### Field | Input Value
--- | ---
**Claim Status** | Outcomes:
- **N/A**: There are no claims on the record (no need to review)
- **Won conflict**: The loading application loaded the file but is in conflict with the previously loaded file. Recommendation: Review the two versions of the file to confirm your intended outcome.
- **No conflict**: There may be one or more applications loading but there is no conflict. However, it is still good to review the outcome to see if it's what you intended.
- **Lost conflict**: The file was not loaded because another application has a better claim on the file. Recommendation: Review the two versions of the file to see which should be loaded (or if they should be merged).

**Priority** | Relative importance of the conflict that caused the skip based on the following criteria:
- **1**: UI pages, UI macros, and more
- **2**: Business rules, security ACLs, and more
- **3**: Reports and more
- **4**: Form sections, choice sets, and more
- **5**: Everything else

**Resolution** | • Not reviewed: Records which have not been reviewed
- **Reviewed**: Records which have been reviewed
- **Reviewed and Merged**: Records which have been reviewed and have both the old and new changes
- **Reviewed and Retained**: Records which have been reviewed and have retained the updates from the latest upgrade
- **Reviewed and Reverted**: Records which have been reviewed and have reverted changes to the base system

**Comment** | During the process of resolving a skipped update, you have the option to add a **Comment** to any record. For example, the comment might explain the action that you took to future reviewers.

**Target name** | Name of the record corresponding to the current file.

**Plugin** | Plugin that contains the record.

**Type** | Current file type (such as Business Rule or UI Policy).

**Table** | Table that contains the record.

---

**Resolve a skipped update and set a resolution status**

To prevent your customizations from being overwritten during system upgrades, the upgrade process skips (does not apply the update to) objects that have been customized. One of your responsibilities as the administrator is to resolve each skipped update after an upgrade.

Role required: admin

You resolve an update by either retaining the customization or (when the software upgrade contains a feature that you would like to implement) by merging or overwriting the customization with the base system update.
When an object is customized, the system adds a corresponding record to the Customer Updates [sys_update_xml] table and then maintains current version information for all customized objects. The upgrade process skips changes to objects that have a current version in the Customer Updates table. When you follow the procedure, you perform one of the following actions:

- Retain (keep) a customization with no changes
- Retain a customization by merging changes from the updated object
- Revert a customized object to the updated version (that is, overwrite the customization)
- Review the skip and perform no action on the object

1. Navigate to **System Diagnostics > Upgrade History**.
2. Select the desired software version.
3. In the **Skipped Changes to Review related list**, select the update record to resolve.

4. Review the list of changes. For text fields, you can click in the field to open the Diff/Merge tool. Review the differences. Click a text box to view and edit the detailed differences.
5. Perform one of the following actions. You have the option to add a **Comment** to any record, for example, to explain the action to future reviewers.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retain the customized record as is and do not update it.</td>
<td>After reviewing the changes, set Resolution Status to Reviewed and Retained.</td>
</tr>
<tr>
<td></td>
<td>The record moves from the Skipped Changes to Review to Skipped Changes Reviewed related list.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Retain the customization by merging changes from the updated object.</th>
<th>a. Click Resolve Conflicts to navigate to the Resolve Conflicts form.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>b. Review the differences.</td>
</tr>
<tr>
<td></td>
<td>c. To merge a field:</td>
</tr>
<tr>
<td></td>
<td>• Click the right-arrow button for the field.</td>
</tr>
<tr>
<td></td>
<td>• Click a text box to view and edit the detailed differences.</td>
</tr>
<tr>
<td></td>
<td>• When you have merged all appropriate fields, click Merge.</td>
</tr>
</tbody>
</table>

After merging the customization changes:

- The Resolution Status changes to Reviewed and Merged.
- The record moves from the Skipped Changes to Review to the Skipped Changes Reviewed related list.
<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Discard the customization and update the record to match the base system for this upgrade. | After reviewing the changes, click **Revert to Base System**.  
  - The **Disposition** changes from **Skipped** to **Reverted**.  
  - The **Resolution Status** changes to **Reviewed and Reverted**.  
  - The system creates a Customer Update record.  
  - The record moves from the Skipped Changes to Review to the Skipped Changes Reviewed related list. |

**Note**: At any time after you revert a customization, you can click **Reapply Changes** to reapply the customization (undo the revert).

| Review the skip and perform no action on the object. | After reviewing the changes, set **Resolution Status** to **Reviewed**. The record moves from the Skipped Changes to Review to the Skipped Changes Reviewed related list. |
| Leave on the skipped list for a later decision, and note that you have not reviewed the record. | From the **Resolution** list, choose **Not Reviewed** to defer the decision on how to handle this conflict. The record stays on the Skipped Changes to Review related list. |

6. Click **Update**. Repeat the process to resolve each update record in the list.

Only skipped updates with a **Resolution Status** of **Not Reviewed** or a resolution set appear in the Skipped Changes to Review related list. Any action you take that changes the **Resolution Status** to a value other than **Not Reviewed** or **--None--** removes the skipped update from the list and moves it to the Skipped Changes Reviewed related list.

**Skipped Changes Reviewed related list**

Skipped Changes Reviewed lists update records that previously appeared on the Skipped Changes to Review related list and have been reviewed. When you select a skipped record to review and set a **Resolution Status** to a value other than **Not Reviewed**, the update record moves to the Skipped Changes Reviewed related list.

Navigate to **System Diagnostics > Upgrade History** to view the Skipped Changes Reviewed related list.

**Skipped Changes Reviewed related list**

<table>
<thead>
<tr>
<th>Field</th>
<th>Input Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>File name</td>
<td>Name of reviewed Upgrade Details record.</td>
</tr>
<tr>
<td>Field</td>
<td>Input Value</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Disposition</strong></td>
<td>Action performed on this file during the selected upgrade:</td>
</tr>
<tr>
<td></td>
<td>• Inserted: The system inserted a new record.</td>
</tr>
<tr>
<td></td>
<td>• Updated: The system updated this record.</td>
</tr>
<tr>
<td></td>
<td>• Deleted: The system deleted this record.</td>
</tr>
<tr>
<td></td>
<td>• Skipped: The system did not change this record in order to preserve customizations.</td>
</tr>
<tr>
<td></td>
<td>• Reverted: This record was reverted to the base version.</td>
</tr>
<tr>
<td></td>
<td>• Table not found: The system could not find the table that contains this record.</td>
</tr>
<tr>
<td></td>
<td>• Unchanged: The system did not change this record because the baseline component has not changed since the last release.</td>
</tr>
<tr>
<td></td>
<td>• Skipped Manual Merge: The system did not change this record because updating it requires manual intervention.</td>
</tr>
<tr>
<td></td>
<td>• Skipped Apply Once: The system skipped this record because it had already applied an update from an xml file in the apply once folder.</td>
</tr>
<tr>
<td></td>
<td>• Not Latest: The system applied a change, but this change was overwritten later during the same upgrade.</td>
</tr>
<tr>
<td><strong>Claim Status</strong></td>
<td><strong>Outcomes:</strong></td>
</tr>
<tr>
<td></td>
<td>• N/A: There are no claims on the record (no need to review)</td>
</tr>
<tr>
<td></td>
<td>• Won conflict: The loading application loaded the file but is in conflict with the previously loaded file. Recommendation: Review the two versions of the file to confirm your intended outcome.</td>
</tr>
<tr>
<td></td>
<td>• No conflict: There may be one or more applications loading but there is no conflict. However, it is still good to review the outcome to see if it's what you intended.</td>
</tr>
<tr>
<td></td>
<td>• Lost conflict: The file was not loaded because another application has a better claim on the file. Recommendation: Review the two versions of the file to see which should be loaded (or if they should be merged).</td>
</tr>
<tr>
<td><strong>Priority</strong></td>
<td>Relative importance of the conflict that caused the skip based on the following criteria:</td>
</tr>
<tr>
<td></td>
<td>• 1 (highest priority): xml content</td>
</tr>
<tr>
<td></td>
<td>• 2: script or script_plain</td>
</tr>
<tr>
<td></td>
<td>• 3: html content</td>
</tr>
<tr>
<td></td>
<td>• 4: sys_ui_form_section, sys_ui_related_list, or sys_choice_set</td>
</tr>
<tr>
<td></td>
<td>• 5 (lowest priority): other</td>
</tr>
<tr>
<td><strong>Resolution</strong></td>
<td>• Reviewed</td>
</tr>
<tr>
<td></td>
<td>• Retained</td>
</tr>
<tr>
<td></td>
<td>• Reverted</td>
</tr>
<tr>
<td><strong>Comment</strong></td>
<td>During the process of resolving a skipped update, you have the option to add a Comment to any record. For example, the comment might explain the action that you took to future reviewers.</td>
</tr>
</tbody>
</table>
### Customizations Unchanged related list

Customizations Unchanged lists all records that were skipped (due to a customization), but the changes that were going to be applied in this upgrade have not changed from the last upgrade.

Navigate to **System Diagnostics > Upgrade History** to view the Customizations Unchanged related list.

<table>
<thead>
<tr>
<th>Field</th>
<th>Input Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>File name</td>
<td>Name of unchanged sys_upgrade_history_log record. Select it if you want to access Upgrade Details and add comment text, or set a resolution status for it.</td>
</tr>
<tr>
<td>Disposition</td>
<td>Action performed on this file during the selected upgrade:</td>
</tr>
<tr>
<td></td>
<td>• Inserted: The system inserted a new record.</td>
</tr>
<tr>
<td></td>
<td>• Updated: The system updated this record.</td>
</tr>
<tr>
<td></td>
<td>• Deleted: The system deleted this record.</td>
</tr>
<tr>
<td></td>
<td>• Skipped: The system did not change this record in order to preserve customizations.</td>
</tr>
<tr>
<td></td>
<td>• Reverted: This record was reverted to the base version.</td>
</tr>
<tr>
<td></td>
<td>• Table not found: The system could not find the table that contains this record.</td>
</tr>
<tr>
<td></td>
<td>• Unchanged: The system did not change this record because the baseline component has not changed since the last release.</td>
</tr>
<tr>
<td></td>
<td>• Skipped Manual Merge: The system did not change this record because updating it requires manual intervention.</td>
</tr>
<tr>
<td></td>
<td>• Skipped Apply Once: The system skipped this record because it had already applied an update from an xml file in the apply once folder.</td>
</tr>
<tr>
<td></td>
<td>• Not Latest: The system applied a change, but this change was overwritten later during the same upgrade.</td>
</tr>
</tbody>
</table>
### Revert a customization

To prevent customizations from being overwritten by system upgrades, the upgrade process automatically skips changes to objects that have been customized. You may want to overwrite your customizations when a software upgrade contains a feature that you would like to implement.

**Role required:** admin

To identify customized objects, the system adds a corresponding record in the Customer Updates [sys_update_xml] table. The table maintains the current version information for all objects that have been customized. The upgrade process skips changes to objects that have entries in the table. The upgrade process does not skip objects if only excluded fields have changed.

1. Navigate to **System Diagnostics > Upgrade History**.
2. Select the desired software version.
3. Filter the Upgrade Details related list by **Disposition is Skipped**.
4. Optional: Add another filter condition for **Changed is True** to return only the objects that have changed since the last upgrade.
5. Select the update record to implement.
   - The **File differences** field displays a side-by-side comparison of the customization and the default version. Deletions are highlighted in red, additions in green, and modifications in yellow.
6. Click **Revert to base system** to overwrite your customized object with the system default version.
   - The **Disposition** changes from **Skipped** to **Reverted**.
   - After you revert a customization, you have the option to click **Reapply Changes** to reapply your customizations (undo the revert).

<table>
<thead>
<tr>
<th>Field</th>
<th>Input Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Relative importance of the conflict that caused the skip based on the following criteria:</td>
</tr>
<tr>
<td></td>
<td>• 1 (highest priority): xml content</td>
</tr>
<tr>
<td></td>
<td>• 2: script or script_plain</td>
</tr>
<tr>
<td></td>
<td>• 3: html content</td>
</tr>
<tr>
<td></td>
<td>• 4: sys_ui_form-section, sys_ui_related_list, or sys_choice_set</td>
</tr>
<tr>
<td></td>
<td>• 5 (lowest priority): other</td>
</tr>
<tr>
<td>Resolution</td>
<td>• Reviewed</td>
</tr>
<tr>
<td></td>
<td>• Retained</td>
</tr>
<tr>
<td></td>
<td>• Reverted</td>
</tr>
<tr>
<td>Comment</td>
<td>During the process of resolving a skipped update, you have the option to add a Comment to any record. For example, the comment might explain the action that you took to future reviewers.</td>
</tr>
<tr>
<td>Changed by vendor</td>
<td>Indicates whether the file has been changed by the vendor since the last upgrade.</td>
</tr>
<tr>
<td>Target name</td>
<td>Name of the record corresponding to the current file.</td>
</tr>
<tr>
<td>Plugin</td>
<td>Plugin that contains the record.</td>
</tr>
<tr>
<td>Type</td>
<td>Current file type (such as Business Rule or UI Policy).</td>
</tr>
<tr>
<td>Table</td>
<td>Table that contains the record.</td>
</tr>
</tbody>
</table>
## Changes Applied related list

Changes Applied lists all changes that were applied in this upgrade.

This list is ordered by priority and displays Upgrade Detail records for this upgrade that have a disposition of Updated, Updated (second pass), Inserted, Inserted (second pass), Deleted, Deleted (second pass), and for which the changed flag is true for all of the dispositions.

Navigate to **System Diagnostics > Upgrade History** to view the Changes Applied related list.

### Changes Applied related list

<table>
<thead>
<tr>
<th>Field</th>
<th>Input Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disposition</td>
<td>Action performed on this file during the selected upgrade:</td>
</tr>
<tr>
<td></td>
<td>• Inserted: The system inserted a new record.</td>
</tr>
<tr>
<td></td>
<td>• Updated: The system updated this record.</td>
</tr>
<tr>
<td></td>
<td>• Deleted: The system deleted this record.</td>
</tr>
<tr>
<td></td>
<td>• Skipped: The system did not change this record in order to preserve customizations.</td>
</tr>
<tr>
<td></td>
<td>• Reverted: This record was reverted to the base version.</td>
</tr>
<tr>
<td></td>
<td>• Table not found: The system could not find the table that contains this record.</td>
</tr>
<tr>
<td></td>
<td>• Unchanged: The system did not change this record because the baseline component has not changed since the last release.</td>
</tr>
<tr>
<td></td>
<td>• Skipped Manual Merge: The system did not change this record because updating it requires manual intervention.</td>
</tr>
<tr>
<td></td>
<td>• Skipped Apply Once: The system skipped this record because it had already applied an update from an xml file in the apply once folder.</td>
</tr>
<tr>
<td></td>
<td>• Not Latest: The system applied a change, but this change was overwritten later during the same upgrade.</td>
</tr>
<tr>
<td>Priority</td>
<td>Relative importance of the conflict that caused the skip based on the following criteria:</td>
</tr>
<tr>
<td></td>
<td>• 1 (highest priority): xml content</td>
</tr>
<tr>
<td></td>
<td>• 2: script or script_plain</td>
</tr>
<tr>
<td></td>
<td>• 3: html content</td>
</tr>
<tr>
<td></td>
<td>• 4: sys_ui_form_section, sys_ui_related_list, or sys_choice_set</td>
</tr>
<tr>
<td></td>
<td>• 5 (lowest priority): other</td>
</tr>
<tr>
<td>Resolution</td>
<td>• Reviewed</td>
</tr>
<tr>
<td></td>
<td>• Retained</td>
</tr>
<tr>
<td></td>
<td>• Reverted</td>
</tr>
<tr>
<td>Comment</td>
<td>During the process of resolving a skipped update, you have the option to add a <strong>Comment</strong> to any record. For example, the comment might explain the action that you took to future reviewers.</td>
</tr>
<tr>
<td>Target name</td>
<td>Name of the record corresponding to the current file.</td>
</tr>
<tr>
<td>Plugin</td>
<td>Plugin that contains the record.</td>
</tr>
<tr>
<td>Type</td>
<td>Current file type (such as Business Rule or UI Policy).</td>
</tr>
</tbody>
</table>
Claim Outcomes to Review related list

During system upgrades, the Claim Status tab displays outcomes to review and resolve. See the Claim Status field in the table below.

By default, the list is filtered by Disposition Skipped Error, Disposition Skipped Manual Merge, Disposition Skipped, or Disposition Skipped (second pass), and the resolution status is either empty or not reviewed.

Navigate to System Diagnostics > Upgrade History to view the Claimed Outcomes to Review related list.

<table>
<thead>
<tr>
<th>Field</th>
<th>Input Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>Table that contains the record.</td>
</tr>
<tr>
<td>File name</td>
<td>Current upgrade file name.</td>
</tr>
<tr>
<td>File differences</td>
<td>Comparison of the file in the upgrade with the customized version.</td>
</tr>
<tr>
<td>Changed by vendor</td>
<td>Indicates whether the file has been changed by the vendor since the last upgrade.</td>
</tr>
</tbody>
</table>

Claimed Outcomes to Review related list

<table>
<thead>
<tr>
<th>Field</th>
<th>Input Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>File name</td>
<td>Name of skipped Upgrade Detail record.</td>
</tr>
<tr>
<td>Disposition</td>
<td>Action performed on this file during the selected upgrade:</td>
</tr>
<tr>
<td></td>
<td>• Inserted: The system inserted a new record.</td>
</tr>
<tr>
<td></td>
<td>• Updated: The system updated this record.</td>
</tr>
<tr>
<td></td>
<td>• Deleted: The system deleted this record.</td>
</tr>
<tr>
<td></td>
<td>• Skipped: The system did not change this record in order to preserve customizations.</td>
</tr>
<tr>
<td></td>
<td>• Reverted: This record was reverted to the base version.</td>
</tr>
<tr>
<td></td>
<td>• Table not found: The system could not find the table that contains this record.</td>
</tr>
<tr>
<td></td>
<td>• Unchanged: The system did not change this record because the baseline component has not changed since the last release.</td>
</tr>
<tr>
<td></td>
<td>• Skipped Manual Merge: The system did not change this record because updating it requires manual intervention.</td>
</tr>
<tr>
<td></td>
<td>• Skipped Apply Once: The system skipped this record because it had already applied an update from an xml file in the apply once folder.</td>
</tr>
<tr>
<td></td>
<td>• Not Latest: The system applied a change, but this change was overwritten later during the same upgrade.</td>
</tr>
<tr>
<td>Field</td>
<td>Input Value</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Claim Status</td>
<td>Outcomes:</td>
</tr>
<tr>
<td></td>
<td>• N/A: There are no claims on the record (no need to review)</td>
</tr>
<tr>
<td></td>
<td>• Won conflict: The loading application loaded the file but is in conflict with the previously loaded file. Recommendation: Review the two versions of the file to confirm your intended outcome.</td>
</tr>
<tr>
<td></td>
<td>• No conflict: The installing application loaded the file without any conflicts; however, there may be one or more applications loading the same file so it is still recommended to review the outcomes.</td>
</tr>
<tr>
<td></td>
<td>• Lost conflict: The file was not loaded because another application has a better claim on the file. Recommendation: Review the two versions of the file to see which should be loaded (or if they should be merged).</td>
</tr>
<tr>
<td>Priority</td>
<td>Relative importance of the conflict that caused the skip based on the following criteria:</td>
</tr>
<tr>
<td></td>
<td>• 1: UI pages, UI macros, and more</td>
</tr>
<tr>
<td></td>
<td>• 2: Business rules, security ACLs, and more</td>
</tr>
<tr>
<td></td>
<td>• 3: Reports and more</td>
</tr>
<tr>
<td></td>
<td>• 4: Form sections, choice sets, and more</td>
</tr>
<tr>
<td></td>
<td>• 5 Everything else</td>
</tr>
<tr>
<td>Resolution</td>
<td>• Not reviewed: Records which have not been reviewed</td>
</tr>
<tr>
<td></td>
<td>• Reviewed: Records which have been reviewed</td>
</tr>
<tr>
<td></td>
<td>• Reviewed and Merged: Records which have been reviewed and have both the old and new changes</td>
</tr>
<tr>
<td></td>
<td>• Reviewed and Retained: Records which have been reviewed and have retained the updates from the latest upgrade</td>
</tr>
<tr>
<td></td>
<td>• Reviewed and Reverted: Records which have been reviewed and have reverted changes to the base system</td>
</tr>
<tr>
<td>Comment</td>
<td>During the process of resolving a skipped update, you have the option to add a Comment to any record. For example, the comment might explain the action that you took to future reviewers.</td>
</tr>
<tr>
<td>Target name</td>
<td>Name of the record corresponding to the current file.</td>
</tr>
<tr>
<td>Plugin</td>
<td>Plugin that contains the record.</td>
</tr>
<tr>
<td>Type</td>
<td>Current file type (such as Business Rule or UI Policy).</td>
</tr>
<tr>
<td>Table</td>
<td>Table that contains the record.</td>
</tr>
</tbody>
</table>

**Upgrade Details related list**

Upgrade Details lists all Upgrade Details records for this upgrade.

Navigate to **System Diagnostics > Upgrade History** to view the Upgrade Details related list.
## Upgrade Details related list

<table>
<thead>
<tr>
<th>Field</th>
<th>Input Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disposition</td>
<td>Action performed on this file during the selected upgrade:</td>
</tr>
<tr>
<td></td>
<td>• Inserted: The system inserted a new record.</td>
</tr>
<tr>
<td></td>
<td>• Updated: The system updated this record.</td>
</tr>
<tr>
<td></td>
<td>• Deleted: The system deleted this record.</td>
</tr>
<tr>
<td></td>
<td>• Skipped: The system did not change this record in order to preserve customizations.</td>
</tr>
<tr>
<td></td>
<td>• Reverted: This record was reverted to the base version.</td>
</tr>
<tr>
<td></td>
<td>• Table not found: The system could not find the table that contains this record.</td>
</tr>
<tr>
<td></td>
<td>• Unchanged: The system did not change this record because the baseline component has not changed since the last release.</td>
</tr>
<tr>
<td></td>
<td>• Skipped Manual Merge: The system did not change this record because updating it requires manual intervention.</td>
</tr>
<tr>
<td></td>
<td>• Skipped Apply Once: The system skipped this record because it had already applied an update from an xml file in the apply once folder.</td>
</tr>
<tr>
<td></td>
<td>• Not Latest: The system applied a change, but this change was overwritten later during the same upgrade.</td>
</tr>
<tr>
<td>Priority</td>
<td>Relative importance of the conflict that caused the skip based on the following criteria:</td>
</tr>
<tr>
<td></td>
<td>• 1 (highest priority): xml content</td>
</tr>
<tr>
<td></td>
<td>• 2: script or script_plain</td>
</tr>
<tr>
<td></td>
<td>• 3: html content</td>
</tr>
<tr>
<td></td>
<td>• 4: sys_ui_form_section, sys_ui_related_list, or sys_choice_set</td>
</tr>
<tr>
<td></td>
<td>• 5 (lowest priority): other</td>
</tr>
<tr>
<td>Claim Status</td>
<td>Outcomes:</td>
</tr>
<tr>
<td></td>
<td>• N/A: There are no claims on the record (no need to review)</td>
</tr>
<tr>
<td></td>
<td>• Won conflict: The loading application loaded the file but is in conflict with the previously loaded file. Recommendation: Review the two versions of the file to confirm your intended outcome.</td>
</tr>
<tr>
<td></td>
<td>• No conflict: There may be one or more applications loading but there is no conflict. However, it is still good to review the outcome to see if it's what you intended.</td>
</tr>
<tr>
<td></td>
<td>• Lost conflict: The file was not loaded because another application has a better claim on the file. Recommendation: Review the two versions of the file to see which should be loaded (or if they should be merged).</td>
</tr>
<tr>
<td>Resolution</td>
<td>• Reviewed</td>
</tr>
<tr>
<td></td>
<td>• Retained</td>
</tr>
<tr>
<td></td>
<td>• Reverted</td>
</tr>
</tbody>
</table>
### Upgrade Monitor module: Upgrade an individual instance

The Upgrade Monitor helps you upgrade an individual instance. You can monitor the progress of an upgrade and resolve conflicts between the upgrade and customizations.

#### Set up

- Upgrade Monitor overview

#### Use

- Monitor an upgrade to an instance
- Process the skipped records list
- Resolve conflicts for an individual record

#### Troubleshoot and get help

- Debug upgrade for last upgrade session.
- Ask or answer questions in the Developer Community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

---

### Upgrade Monitor overview

The Upgrade Monitor helps you upgrade an individual instance. You can monitor the progress of an upgrade and resolve conflicts between the upgrade and customizations.

### Set up for the Upgrade Monitor

In Quebec, the Upgrade Monitor is installed by default.

If you log in with the admin role while an upgrade is underway, the system automatically displays the Upgrade Progress screen. If no upgrade is in progress, you can navigate to **System Diagnostics > Upgrade Monitor**.

### How the Upgrade Monitor fits into the upgrade process

**Note:** For detailed information about the upgrade process, see Upgrade your instance.

The Upgrade Monitor concerns only part of the larger upgrade process:

1. Clone the production instance to a test instance and a non-production instance.
2. Apply the upgrade to the non-production instance.

3. On the upgraded non-production instance, process the skipped list.

4. Test the non-production instance to confirm that the instance still works and performs adequately. Compare to benchmark data from pre-upgrade production instance.

5. Apply the upgrade to the test instance. Import the update sets created on the non-production instance when you processed the skipped list. Repeat the testing to make sure that the process is working.

6. Apply the upgrade to the production instance. Import the update sets created on the non-production instance when you processed the skipped list. Test to confirm that the instance works and performs adequately.

Within this larger process, the Upgrade Monitor helps you upgrade individual instances:

- during the upgrade, it shows where in the process the system is
- after the upgrade, it reports what the upgrade did and for how long
- as you upgrade the first non-production instance, it helps you resolve conflicts between customizations and changes that are part of the upgrade
- on non-production instances, it provides information that can help you estimate how long the upgrade takes on the production instance.

**Note:** Debug Upgrade provides detailed debugging output for transactions containing artifacts affected by the most recent upgrade, and is designed to assist in upgrade error resolution. See Debug upgrade.

**Monitoring an individual instance as it upgrades**

While the upgrade is in progress the Upgrade Progress shows what the upgrade process has done, what it is doing, and what remains to be done.

When the upgrade completes, the system displays the Upgrade Summary Report. The Upgrade Summary Report provides information about conflicts between customizations versus the upgrade and provides a link to reconcile these conflicts. For information about understanding and resolving these conflicts, see Process the skipped records list.

When you upgrade a non-production instance, the Upgrade Summary Report can help you estimate how long the same upgrade takes on a production instance. For details about the elements on this report and how to use this information, see Upgrade Details form.

**Resolving conflicts**

To prevent losing customizations, the system skips upgrading records you have customized and provides you with a list of these skipped records.

As you upgrade your first non-production instance, go through the Skipped Changes to Review related list and resolve these conflicts. The system records the changes you make during this process in update sets.

You do not need to reconcile the skipped list on any instances you later upgrade. Instead, you can apply the upgrade then import the update sets containing your changes.

For details on reconciling conflicts, see Process the skipped records list.

**Factors affecting upgrade duration**

Various factors affect how long the system takes to perform an upgrade. The Upgrade Monitor can help you understand those factors and estimate how long the upgrade to your production instance takes.

Many factors can affect the duration of the upgrade process:
• The number of records in the database
• The number of customizations in the database
• The number of nodes in the instance
• The size of tables in the instance that require a schema-change in the instance.
• The number of fix scripts required and the size of the tables those fix scripts manipulate.

Upgrading a non-production instance can help you estimate how long the upgrade takes on production, but differences between the instances can significantly affect the duration:

• When you cloned the production instance to the non-production instance, you may have clone-excluded some tables. This reduces the size of the database and makes the non-production instance upgrade faster than the production instance.
• The production instance may have more memory and processing power.
• The production instance may have more nodes than the non-production instance.

After upgrading the first non-production instance, examine the Upgrade Summary Report for data to help estimate the impact of these factors.

Note: The performance of the upgrade engine is significantly enhanced and optimized for all types of upgrades (in-family, and family-to-family) in Madrid and later releases.

Upgrade Monitor

When an upgrade is not running, the Upgrade Monitor displays information about the next check for an available upgrade.

The Upgrade Monitor displays the next date and time when the system will check for an available upgrade.
To check immediately for an available upgrade, click **Check Now**.

If one or both of the triggers for upgrading the system ('Check distribution for possible upgrade' and 'Check database for possible upgrade') have been customized or are missing, the Upgrade Monitor displays a warning and provides a button for resolving the issues.

**Note:** If your instance is self-hosted (not hosted by ServiceNow) this message may not necessarily indicate a problem. If you have customized or disabled the upgrade job and want to keep that customization or disabled state, do not click the button to fix the upgrade issue.

**Upgrade Monitor with Issue Detected**

To resolve the issues with the upgrade jobs, click **Fix Upgrade Jobs**. This action reverts both upgrade triggers ('Check distribution for possible upgrade' and 'Check database for possible upgrade') to their base versions.

**Note:** 'Upgrade' job has been renamed to 'Check distribution for possible upgrade' starting Paris. 'Check Upgrade Script' job has been renamed to 'Check database for possible upgrade' starting Paris.
Monitor an upgrade to an instance

While the system is upgrading an instance, you can monitor its progress with the Upgrade Monitor. When the upgrade is done, you can view a summary of the results on the Upgrade Summary Report.

1. If necessary, navigate to System Diagnostics > Upgrade Monitor.
   - When an upgrade is in progress, the Upgrade Progress page shows its status.
2. Monitor the progress of the upgrade.
   - When the system finishes the upgrade, it displays the Upgrade Summary Report.

From the Upgrade Summary Report, resolve any conflicts that prevented the system from upgrading records.

Upgrade Progress

When an upgrade is underway, Upgrade Progress displays progress bars and other information to help monitor the process.
### Screen elements

<table>
<thead>
<tr>
<th>Screen element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade Progress</td>
<td>A progress bar depicting where the upgrade is in the overall process. The length of a section in the bar does not indicate the relative duration of that process.</td>
</tr>
<tr>
<td>Upgrade Progress: Upgrading Platform</td>
<td>The system is applying upgrades to elements that form the foundation of the platform.</td>
</tr>
<tr>
<td>Upgrade Progress: Updating Schema</td>
<td>The system is scanning the plugins to create a list of tables that require upgrading. This prevents the system from upgrading the same table multiple times.</td>
</tr>
<tr>
<td>Upgrade Progress: Loading Plugins</td>
<td>The system is loading both core and optional plugins. Some features require more than one plugin, so the number of plugins listed may not match the number of optional features installed.</td>
</tr>
<tr>
<td>Upgrade Progress: Completing</td>
<td>The system is upgrading components that need to be completed after the previous three stages are done.</td>
</tr>
</tbody>
</table>

**Note:** After the system finishes the Completing phase, it displays a separate screen showing Finalizing. The system tracks in update sets the changes made during the Upgrading Platform, Updating Schema, Loading Plugins, and Completing phases. It does not track changes made during Finalizing.

<table>
<thead>
<tr>
<th>Details</th>
<th>Shows the current activity, a progress bar for the current activity, and the file currently being updated.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node Upgrades</td>
<td>The color of the icons represents the status of each node during this upgrade: Pending, Running, Successful, Failed, or Down.</td>
</tr>
<tr>
<td>Node</td>
<td>The selected node indicated by the arrow. To change the selection, position the mouse cursor over the icon for the node to select.</td>
</tr>
<tr>
<td>Running time</td>
<td>How long the selected node (indicated by the arrow) has been running. If the selected node is offline, this value stops updating and shows how long a node was online before going offline.</td>
</tr>
<tr>
<td>Version</td>
<td>The current build for the selected node (indicated by the arrow).</td>
</tr>
<tr>
<td>Successful upgrade</td>
<td>When the selected node is online, shows how long the node has been online. If the selected node is offline, shows how long the node has been offline.</td>
</tr>
</tbody>
</table>
Upgrade Summary Report

This report summarizes the actions taken, provides tools to resolve conflicts between customizations and the upgrade, and provides information to help estimate time for upgrades to other instances.

Upgrade Summary Report: Database Upgrade Highlights

<table>
<thead>
<tr>
<th>Screen element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From version</td>
<td>Previous version of the instance</td>
</tr>
<tr>
<td>To version</td>
<td>Upgraded version of the instance</td>
</tr>
<tr>
<td>Started</td>
<td>When the upgrade process started</td>
</tr>
<tr>
<td>Finished</td>
<td>When the upgrade process finished</td>
</tr>
<tr>
<td>Duration</td>
<td>How long the upgrade process took</td>
</tr>
<tr>
<td>Screen element</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Skipped</td>
<td>In the example, 24 Skipped of 7016 changes reads as:</td>
</tr>
<tr>
<td></td>
<td>• <strong>24 Skipped</strong> - Total number of customizations that were skipped, skipped manual merge, or skipped in error, and the file changed in the distribution since the last upgrade of the instance. These are the number of records the system did not upgrade because of conflicts between customizations and the upgrade.</td>
</tr>
<tr>
<td></td>
<td>• <strong>7016 Changes</strong> - Total number of file changes in the distribution since the last upgrade of the instance, plus all inserts and deletes.</td>
</tr>
<tr>
<td></td>
<td>Note: The manner in which upgrade records are counted was changed in the Jakarta release, which may render different record counts than in previous releases.</td>
</tr>
<tr>
<td>Review Skipped Updates</td>
<td>Click to reconcile conflicts that caused the system to skip some updates</td>
</tr>
</tbody>
</table>

**Node Upgrades**

![Node Upgrades](image)

The Node Upgrades section shows the status of the upgrade for each node in the instance. The color of the icon denotes the status, as illustrated by the legend (key) and to the right of the node icons. To see details about a node, position the cursor above the icon for that node. An arrow points to the node selected, and the information below the icons pertains to that node.

**Upgrade Summary Report: Node Upgrades**

The Node Upgrades section shows the status of the upgrade for each node in the instance. The color of the icon denotes the status, as illustrated by the legend (key) and to the right of the node icons. To see details about a node, position the cursor above the icon for that node. An arrow points to the node selected, and the information below the icons pertains to that node.
Schema Changes to Clone-excluded Tables

Upgrade Summary Report: Schema Changes to Clone-excluded tables

The Schema Changes to Clone-excluded Tables section shows a list of tables affected by the upgrade that were clone-excluded when you cloned the production instance to this instance. Because clone-excluded tables are empty, upgrading them takes less time than upgrading those same tables on the production instance. To estimate how much longer the production upgrade takes, note the size of the clone-excluded tables on the production instance.
Top 10 Fix Scripts by Duration

<table>
<thead>
<tr>
<th>Duration</th>
<th>Name / Description</th>
<th>Duration</th>
<th>Name / Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Minute</td>
<td>fix_promote_cmdb_attributes_to_cmdb.xml repair cmdb_ui is cmdb</td>
<td>21 Seconds</td>
<td>activate_amb_plugin.xml</td>
</tr>
<tr>
<td>1 Minute</td>
<td>ez_fix_index_for_identification.xml creates database indices for out-of-the-box</td>
<td>20 Seconds</td>
<td>ez_syslog_transaction_schema_change.xml Add the ACL field to syslog_transaction</td>
</tr>
<tr>
<td></td>
<td>identification rules</td>
<td></td>
<td>without long after</td>
</tr>
<tr>
<td>31 Seconds</td>
<td>ez_metadata_conversion_6.xml Metadata conversion re-parenting</td>
<td>12 Seconds</td>
<td>activate_live_upgrade_plugin.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Load the Live Upgrade plugin early, to ensure feature upon first upgrade</td>
</tr>
<tr>
<td>27 Seconds</td>
<td>fix_extended_web_server.xml Move existing records in the web_server table to the</td>
<td>8 Seconds</td>
<td>activate_amb_msg_notification.xml</td>
</tr>
<tr>
<td></td>
<td>new extended web-server tables based on the type of the web server</td>
<td></td>
<td>Activate task notification on sys_amb_message</td>
</tr>
<tr>
<td>25 Seconds</td>
<td>fix_promote_database_application_fields.xml Promote Listener name to Database</td>
<td>7 Seconds</td>
<td>fix_relate_list_calculated_name.xml</td>
</tr>
<tr>
<td></td>
<td>Instance, Edition and is clustered to application</td>
<td></td>
<td>fix_sys_ui_related_list_calculated_name</td>
</tr>
</tbody>
</table>

Click here to see all fix script durations

Upgrade Summary Report: Top 10 Fix Scripts by Duration

The Top 10 Fix Scripts by Duration helps you understand which fix scripts required the most time.
Top 10 Schema Changes by Duration

<table>
<thead>
<tr>
<th>Duration</th>
<th>Table name</th>
<th>Alter Type(s)</th>
<th>Element Names</th>
<th>Flow Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 Seconds</td>
<td>sys_upgrade_history_log</td>
<td>create_indexes</td>
<td>[index1: [upgrade_history, resolution_status, disposition, type_priority, index2: [upgrade_history, order], index3: [ordered]]</td>
<td>33978</td>
</tr>
<tr>
<td>3 Seconds</td>
<td>sys_upgrade_history_log</td>
<td>add_columns</td>
<td>[resolution_status, plugin, type_priority, sys_source_table, comments]</td>
<td>33978</td>
</tr>
<tr>
<td>2 Seconds</td>
<td>sys_upgrade_history_log</td>
<td>modify_column</td>
<td>'file_path' MEDIUMTEXT</td>
<td>33978</td>
</tr>
<tr>
<td>1 Second</td>
<td>rmb_h Ci</td>
<td>modify_column</td>
<td>'correlation_id' MEDIUMTEXT</td>
<td>2752</td>
</tr>
</tbody>
</table>

Upgrade Summary Report: Top 10 Schema Changes by Duration

The Top 10 Schema Changes by Duration helps you understand which schema changes required the most time.

Process the skipped records list

If you customized or altered a record affected by this upgrade, such as a business rule or script, the upgrade generates a skip log record. You must resolve the differences between the upgraded and customized versions of the record by processing the skipped record list, or, in other terms, just processing the skipped list.

Role required: admin

Review the changes you made to baseline records, such as business rules and scripts, that appear on the skipped records list and revert to the baseline version if appropriate. Post-upgrade, thoroughly test all changes you made to these records.

1. If necessary, navigate to System Diagnostics > Upgrade Monitor.
   If the upgrade is still in progress, the system displays the Upgrade Progress screen. When the upgrade finishes, the system displays the Upgrade Summary Report.

2. After the system displays the Upgrade Summary Report, click the Click here link in the Skipped box.
   The system displays the System Upgrades form.


4. Click the row for the first record you want to reconcile.
   The system displays the Upgrade Details form for that record.
5. Evaluate how you want to resolve the conflict for this record and take the appropriate action:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Retain the customized record as is and do not update it.</strong></td>
<td>After reviewing the changes, set Resolution Status to <strong>Reviewed and Retained</strong>. The record moves from the Skipped Changes to Review to Skipped Changes Reviewed related list.</td>
</tr>
</tbody>
</table>
| **Retain the customization by merging changes from the updated object.** | **a.** Click **Resolve Conflicts** to navigate to the Resolve Conflicts form.  
**b.** Review the differences.  
**c.** To merge a field:  
• Click the right-arrow button for the field.  
• Click a text box to view and edit the detailed differences.  
• When you have merged all appropriate fields, click **Merge**.  

After merging the customization changes:  
• The Disposition changes from **Skipped** to **Merged**.  
• The Resolution Status changes to **Reviewed and Merged**.  
• The record moves from the Skipped Changes to Review to the Skipped Changes Reviewed related list. |
| **Discard the customization and update the record to match the base system for this upgrade.** | After reviewing the changes, click **Revert to Base System**.  
• The Disposition changes from **Skipped** to **Reverted**.  
• The Resolution Status changes to **Reviewed and Reverted**.  
• The system creates a Customer Update record.  
• The record moves from the Skipped Changes to Review to the Skipped Changes Reviewed related list. |
| **Review the skip and perform no action on the object.** | After reviewing the changes, set Resolution Status to **Reviewed**. The record moves from the Skipped Changes to Review to the Skipped Changes Reviewed related list. |
| **Leave on the skipped list for a later decision, and note that you have not reviewed the record.** | From the Resolution list, choose **Not Reviewed** to defer the decision on how to handle this conflict. The record stays on the Skipped Changes to Review related list. |

- **Note:** At any time after you revert a customization, you can click **Reapply Changes** to reapply the customization (undo the revert).

- **Note:** The system tracks changes to records in an update set so you can apply these changes to another instance later. However, the system does not migrate the upgrade details records from one instance to the next. These records apply to a specific upgrade of a specific instance. If you want to preserve the Comments, Resolutions, or other information from the skipped list, export it from this instance.
6. In the **Comment** field, write the reasons for making your decision and other information you want to document.

7. Click **Update**.

   Post-upgrade, thoroughly test all changes you made to the records on the skipped record list.

**System Upgrades form**

When an upgrade is complete, the System Upgrades form displays key statistics about the upgrade and a related list of skipped records (the *skipped list*).

![](image)

**Fields**

<table>
<thead>
<tr>
<th>Screen element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From</td>
<td>The version of the instance before upgrading.</td>
</tr>
<tr>
<td>To</td>
<td>The version of the instance after upgrading.</td>
</tr>
<tr>
<td>Upgrade started</td>
<td>The time upgrade started.</td>
</tr>
<tr>
<td>Upgrade finished</td>
<td>The time the upgrade finished.</td>
</tr>
<tr>
<td>Screen element</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Skipped</td>
<td>The number of records the system did not upgrade because of conflicts between customizations and the upgrade.</td>
</tr>
<tr>
<td>Unchanged</td>
<td>The number of records in the instance unchanged by the upgrade.</td>
</tr>
<tr>
<td>Unchanged and customized</td>
<td>The number of customized records in the instance unchanged by the upgrade.</td>
</tr>
<tr>
<td>Skipped error</td>
<td>The number of records the system did not upgrade because of one or more errors.</td>
</tr>
<tr>
<td>Inserted</td>
<td>The number of records the system inserted.</td>
</tr>
<tr>
<td>Updated</td>
<td>The number of records the system successfully updated.</td>
</tr>
<tr>
<td>Deleted</td>
<td>The number of records the system deleted.</td>
</tr>
<tr>
<td>Total</td>
<td>The total number of records the system inspected and/or processed for this upgrade.</td>
</tr>
</tbody>
</table>

### Resolve conflicts for an individual record

Reconcile differences between your customized record and the changes associated with the upgrade.

Role required: admin

1. From the Upgrade Details form for the record you are reconciling, click Resolve Conflicts.
   The system displays the Resolve Conflicts form, which highlights differences between the two versions of the record. The form displays information about the base system record on the left and the customized record on the right.

2. Compare the base system with the customized record for each field on this form. For non-script fields, edit the customized record on the right-hand side to include what you want from the base system and the customization.

3. If this record contains a script, check it for conflicts and resolve.
   a) Click inside the Script field.
      The system displays the Resolve Conflicts - Script form highlighting areas where the two versions of the script differ.
   b) Edit the right-hand side so that the script contains whichever content you want. To move a block of code from the left to right side, click the small arrows corresponding to that block in the middle column.
   c) Click OK.
      The system returns to the Resolve Conflicts form.

4. To save your changes to the record, click Save Merge.
   The system sets the Resolution for this record to Reviewed and Merged.
Upgrade Details form

From the Upgrade Details form, you can review an individual record affected by the upgrade and reconcile conflicts between the upgrade and customizations.

Upgrade Details form

Fields

<table>
<thead>
<tr>
<th>Screen element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File name</td>
<td>The record the system has flagged as needing to be reconciled.</td>
</tr>
<tr>
<td>Screen element</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Priority</td>
<td>The priority the system has assigned to resolving this conflict. Values range from one to five, with one representing the highest priority.</td>
</tr>
<tr>
<td>Comment</td>
<td>Comments to document your decisions about reconciling this record.</td>
</tr>
</tbody>
</table>
| Resolution     | How you elected to resolve this conflict:  
|                | • **Not Reviewed**  
|                | • **Reviewed** - reviewed but no action yet taken  
|                | • **Reviewed and Merged** - made changes to the record to reconcile the customized and upgraded versions  
|                | • **Reviewed and Retained** - left customizations in place without update from upgrade  
|                | • **Reviewed and Reverted** - customizations discarded, record updated according to upgrade  
|                | For more information, see [Process the skipped records list](#). |
| Disposition    | Action performed on this file during the selected upgrade:  
|                | • Inserted: The system inserted a new record.  
|                | • Updated: The system updated this record.  
|                | • Deleted: The system deleted this record.  
|                | • Skipped: The system did not change this record in order to preserve customizations.  
|                | • Reverted: This record was reverted to the base version.  
|                | • Table not found: The system could not find the table that contains this record.  
|                | • Unchanged: The system did not change this record because the baseline component has not changed since the last release.  
|                | • Skipped Manual Merge: The system did not change this record because updating it requires manual intervention.  
|                | • Skipped Apply Once: The system skipped this record because it had already applied an update from an xml file in the apply once folder.  
|                | • Not Latest: The system applied a change, but this change was overwritten later during the same upgrade. |
| Type           | The record type, for example *Script include*. |
| Target name    | Name of the skipped record, if applicable. |
| Update set     | Unused. |
| Plugin         | The plugin containing this record. |
| Table          | The table containing this record. |
### Resolve Conflicts form

The Resolve Conflicts form you compare to the base system version with the customized version of a record and reconcile the differences.

<table>
<thead>
<tr>
<th>Action</th>
<th>Base Systems</th>
<th>Customized</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accessible from</td>
<td>This application scope only</td>
<td>This application scope only</td>
</tr>
<tr>
<td>Active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client viewable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Server side utilities to support add relationship UI.</td>
<td>Server side utilities to support add relationship UI.</td>
</tr>
<tr>
<td>Name</td>
<td>AddRelationshipAjax</td>
<td>AddRelationshipAjax</td>
</tr>
<tr>
<td>Script</td>
<td>var AddRelationshipAjax = Class.create(); AddRelationshipAjax.prototype = Object.extend(ObjectAbstractAjaxProcessor, {</td>
<td>var AddRelationshipAjax = Class.create(); AddRelationshipAjax.prototype = Object.extend(ObjectAbstractAjaxProcessor, {</td>
</tr>
<tr>
<td>Protection policy</td>
<td>None</td>
<td>Read only</td>
</tr>
<tr>
<td>Replace on upgrade</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Fields

The fields this form displays depend on the type of record you are reconciling.

The left column shows the records fields in the base system, including the proposed changes that are part of the upgrade. The right column shows the fields for your customized record.
Debug upgrade

Diagnose and resolve issues you suspect may have resulted from the most recent upgrade by enabling upgrade debugging during a user session. Each transaction lists whether an artifact was skipped, customized by the customer, or modified by ServiceNow during the last family-to-family or patch version upgrade.

Administrators and technical personnel can use this output as an adjunct to the Upgrade History and Upgrade Monitor modules. Debug Upgrade is a component of standard ServiceNow session debugging. You enable Debug Upgrade, process a transaction (for example, load a form), then analyze the reported upgrade information. See Session debug.

Reported debug information

Debug Upgrade includes several expandable sections:

- Skipped During Last Upgrade
- Customer Customized
- ServiceNow Modified During Last Upgrade

These sections serve as a starting point for diagnosing when a function or artifact does not operate as expected after an upgrade. Each listing sorts by the dates the artifacts were processed, with the most recent appearing first. Expand the appropriate section, and click the name of a listed artifact to view the underlying artifact record. These records include update version history, which represents the state of a customizable object at specific times. See Version records.

The listed artifacts may require some kind of possible user intervention or action. Using underlying artifact detail, you can determine:

- what artifacts have changed?
- what artifacts have not been changed that would or should have?
- what changed artifacts were missed?
- what artifacts operate differently than expected (if referencing something that has changed during last upgrade)?

Depending on the answers to these questions, you may have to modify the selected artifact so it works in the way you expect. Conversely, you might simply accept the new updates made to the artifact, and its changed functionality.

Skipped during last upgrade

Lists artifact records that were skipped during the last upgrade that also ran during the last transaction. These records are standard objects that missed changes from ServiceNow because they were modified at some point by a user. See Resolve conflicts for an individual record.

Customer customized

Lists all artifact records that were customized at some point by users that also ran during the last transaction. This listing is not strictly related to the actual activities performed during the last upgrade session. The listing does include the records that appear under Skipped During Last Upgrade. However, not all records that appear in the Customer Customized list are included in Skipped During Last Upgrade.

Note: Customizations that you designate for replacement during upgrades, by setting the Replace on Upgrade field in the customization record to true, do not appear on the Customer Customized section list.

While this listing is not directly related to the activities performed during the last upgrade, it may be worthwhile to look at individual customization records listed on it. Some of the listed customization records may be referencing...
other records changed or skipped during upgrade. The activities performed during the last upgrade may have an impact on, or affect these relationships.

**ServiceNow modified during last upgrade**

Lists all standard (non-customized) artifact records modified by ServiceNow during the last upgrade that also ran during the last transaction.

**Enable and use debug upgrade**

Enable Debug Upgrade to analyze post-upgrade issues that may require follow up, then disable it when finished with the upgrade debugging session.

Role required: admin

1. Navigate to [System Diagnostics > Session Debug](#).
2. Select [Debug Upgrade](#) to enable the upgrade debugger.
3. Process a transaction (for example, load a form).
4. Click the [Skipped During Last Upgrade](#), [Customer Customized](#), or [ServiceNow Modified During Last Upgrade](#) header to view the appropriate list.

<table>
<thead>
<tr>
<th>Upgrade Transaction List</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Field</td>
</tr>
<tr>
<td>---------------</td>
</tr>
<tr>
<td>Type</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Note:</td>
</tr>
</tbody>
</table>

5. The ten most recent artifacts appear in the selected list. Click **Show more** to view all remaining artifacts.
6. Click the name of a listed artifact to view the underlying artifact record.
   For example, if you click a Script Include artifact, the underlying Script Include record appears.
7. To turn off Debug Upgrade and all session debugging after completing your session:
   a) Navigate to **System Diagnostics > Session Debug**.
   b) Select **Disable All** to disable the upgrade debugger.

**Upgrade Center**

Use to plan and manage your upgrades. Use the Upgrade Preview module to explore different release versions available to you and gain insights about the experience of an upgrade without actually upgrading your instance.
You can also monitor the status of any ongoing upgrade and view the summary of your latest upgrade with the new Upgrade Monitor module. The also features an Upgrade visual task board (VTB) to manage post-upgrade skips. A separate Upgrade History module can be used to view all your past upgrades.

**Key features**

**One-stop experience**

You can see all the details that are related to an upgrade.

**Preview your upgrade**

Use the Upgrade Preview module to have an unprecedented insight to an instance prior to an actual or a scheduled upgrade.

You can see the estimated time required to complete an upgrade. The estimated time is calculated from previous upgrades.

**Note:** If this is your first upgrade, **Estimated upgrade duration** doesn't show up.
Reduce post-upgrade review time by previewing the records that have been customized and are different from the upgrade version being previewed and might get skipped due to your customizations in the instance. You can then prioritize your work depending on the records listed in the skip list.

**Monitor an upgrade**

Use the Upgrade Monitor module to schedule and view the status of an ongoing upgrade. You can also reschedule the upgrade by clicking **Reschedule upgrade**. To check for an immediately available upgrade, click **Check for upgrade**.

If an upgrade is in progress, the user is automatically directed to the upgrade in progress page.

**Review previous upgrade detail**

Use the Upgrade History module to view the complete report of any upgrade made to an instance.
You can also view the resolution status of any previous upgrade with skipped records using the visual task board (VTB) view.
Get started

Select the tile to get started.

---

Exploring Upgrade Center

Get an overview of Upgrade Center so you can plan your upgrade ahead.

Upgrade Center helps you plan and manage your upgrades.

- **Previewing an upgrade**: Use the Upgrade Preview module to have an insight about the experience of an upgrade prior to the actual upgrade.
- **Scheduling and monitoring an upgrade**: Use the Upgrade Monitor module to schedule and monitor an upgrade in your instance.
- **Reviewing upgrade history**: Use the Upgrade History module to view reports of completed upgrades in your instance.

Upgrade Preview module

The Upgrade Preview module enables you to have an unprecedented insight to an instance prior to an actual upgrade. You can explore and preview upgrades to different ServiceNow release versions and see how your instance might be impacted with your current configurations. The Upgrade Preview utility helps you to plan, schedule, and prepare for an upgrade.
Find out what's new and changed in Paris Patch 2

Based on your release version, we've provided a list of fixed problems that may be relevant to you. You can also visit the ServiceNow product documentation site to generate personalized release notes, or you can review a list of open known errors on the Known Issue Portal.

Skipped list predictions for an upgrade to Paris Patch 2

When you upgrade to a newer release version, the upgrade can include new features and bug fixes. If customizations are detected during the upgrade, those files are skipped to ensure the upgrade doesn't overwrite any customizations. Here are some predictions of skipped records for an upgrade to the selected release version. Review these predicted skipped records to decide which version of the files you'll like to keep. Before you upgrade, you can also choose to revert some of your customizations to the base version which will send them through the upgrade without getting skipped.

Prepare for your upgrade

Before you upgrade, use the tools below to set a baseline for testing. If you've executed some Automated Test Framework (ATF) tests recently, the most recent results are shown here.

Automated Test Framework (ATF) results

83% Tests passed
**Note:** Depending on the eligibility of your instance, the list of available target versions for preview varies. Only the versions which are allowed for a particular instance to be upgraded to, show up on the list. If your instance is not eligible to be upgraded to any version, the drop down menu will be empty.

The following cards show up with more information.

<table>
<thead>
<tr>
<th>Card names</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current version</td>
<td>Name of the current version.</td>
</tr>
<tr>
<td></td>
<td>• Upgraded on: Date on which the instance got upgraded to the current version</td>
</tr>
<tr>
<td></td>
<td>• End of life: Link to KB0610454 for more information about end of life</td>
</tr>
<tr>
<td>Previewing version</td>
<td>Information about the previewing version show up. If you haven't previewed any version, you are expected to select a version for preview and click Go. If you have already previewed a version, the following information shows up.</td>
</tr>
<tr>
<td></td>
<td>• Preview created: Date on which the preview was created</td>
</tr>
<tr>
<td></td>
<td>• View preview details: Link to the Upgrade Preview form</td>
</tr>
</tbody>
</table>

**Note:** Click **Refresh preview** if you want to regenerate a new preview of the same target version. Although clicking **Refresh preview** regenerates the skipped list, the reverted records won't get skipped. If you have reviewed and retained some records, they get replaced as soon as you click **Refresh preview**.

<table>
<thead>
<tr>
<th>Scheduled upgrade</th>
<th>Name of the next upgrade that has been scheduled to start. If there is no currently scheduled upgrade, the card shows No upgrade scheduled.</th>
</tr>
</thead>
</table>

**Note:** This card can have different messages depending on the schedule of the upgrade.

If there is an upgrade scheduled, the following information shows up.

- Estimated upgrade duration: Estimated duration needed to complete the scheduled upgrade

**Note:** If this is your first upgrade, there will be no information about estimated upgrade duration.

- Next scheduled upgrade: Date and time on which the next upgrade has been scheduled to start.
<table>
<thead>
<tr>
<th>Card names</th>
<th>Description</th>
</tr>
</thead>
</table>
| Find out what's new and changed | Links to view the new and changed features in the current upgrade version. The following three links show up when you click Go to preview the upgrade version.  
  • Problem fixes: Fixes that have been made since the last upgrade version  
  • Personalized release notes: Release notes summary for the previewed version  
  • Known error articles: Errors that have been identified but not yet resolved  |
|                    | Note: These links don't show up if you haven't previewed any upgrades.                                                                      |
| Skipped list prediction | Information about the predicted skipped records. See Preview predicted changes for more details.  
  • Total record changes: Total number of records that are predicted to change when the upgrade occurs. Total record changes also includes possible predicted skip files known as Predicted skipped records.  
    • Review changes: Link to the list of records that have changed and can be reviewed  
    • Predicted skipped records: Total number of records that have been predicted to be skipped.  
    • Total: Total predicted skipped records  
    • To review: Predicted skipped records to be reviewed  
    • Reviewed: Predicted skipped records that have been reviewed  
    • Predicted skipped records by priority: Pie chart to represent the predicted skipped records by priority.  |
|                    | Note: Click the pie chart to take you to the list of predicted skipped records.                                                               |

ServiceNow prioritizes the skipped records based on the importance of the file types. The prioritization is done as follows:  
• Priority 1 (highest priority): UI pages, UI macros, and more  
• Priority 2: Business Rules, Security ACLs, and more  
• Priority 3: Reports and more  
• Priority 4: Form Sections, Choice Sets, and more  
• Priority 5 (lowest priority): everything else
<table>
<thead>
<tr>
<th>Card names</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automated Test Framework (ATF) results</td>
<td>Percentage of passing ATF tests that ran in the last 30 days.</td>
</tr>
<tr>
<td>• Most recent ATF run: Date and time on which the recent ATF tests ran</td>
<td></td>
</tr>
<tr>
<td>• View ATF results: Link to show more information about the recent ATF results</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Only the tests which are finished and have passed are considered for the ATF results. If one test runs more than once, only the recent execution is considered in the results.

---

**Upgrade Monitor module**

Schedule an upgrade and monitor the status of an ongoing upgrade using the Upgrade Monitor module. You can also view the upgrade summary and the list of records causing conflicts in your instance once the upgrade is complete.

**Access Upgrade Monitor**

If you log in with the admin role while an upgrade is underway, the system automatically displays the Upgrade Progress screen. If no upgrade is in progress, you can navigate to **Upgrade Center > Upgrade Monitor**.

**How the Upgrade Monitor fits into the upgrade process**

**Note:** For detailed information about the upgrade process, see **Upgrade your instance**.

The Upgrade Monitor concerns only part of the larger upgrade process:

1. Clone the production instance to a test instance and a non-production instance.
2. Apply the upgrade to the non-production instance.
3. On the upgraded non-production instance, **process the skipped list**.
4. Test the non-production instance to confirm that the instance still works and performs adequately. Compare to benchmark data from pre-upgrade production instance.
5. Apply the upgrade to the test instance. Import the update sets created on the non-production instance when you processed the skipped list. Repeat the testing to make sure that the process is working.
6. Apply the upgrade to the production instance. Import the update sets created on the non-production instance when you processed the skipped list. Test to confirm that the instance works and performs adequately.

Within this larger process, the Upgrade Monitor helps you upgrade individual instances:

- During the upgrade, it shows where in the process the system is
- After the upgrade, it reports what the upgrade did and for how long
- As you upgrade the first non-production instance, it helps you resolve conflicts between customizations and changes that are part of the upgrade
• On non-production instances, it provides information that can help you estimate how long the upgrade might take on the production instance

**Note:** Debug Upgrade provides detailed debugging output for transactions containing artifacts affected by the most recent upgrade, and is designed to assist in upgrade error resolution.

**Monitoring an individual instance as it upgrades**

While the upgrade is in progress the Upgrade Progress shows what the upgrade process has done, what it is doing, and what remains to be done.

When the upgrade completes, the system displays the Upgrade Summary Report. The Upgrade Summary Report provides information about conflicts between customizations versus changes in the upgrade and provides a link to reconcile these conflicts. For information about understanding and resolving these conflicts, see Process the skipped records list.

When you upgrade a non-production instance, the Upgrade Summary Report can help you estimate how long the same upgrade might take on a production instance. For details about the elements on this report and how to use this information, see Upgrade Details form.

**Resolving conflicts**

To prevent losing customizations, the system skips upgrading records you have customized and provides you with a list of these skipped records.

As you upgrade your first non-production instance, go through the Skipped Changes to Review related list and resolve these conflicts. The system records the changes you make during this process in update sets. See Review skipped records using related lists, for more information.

You do not need to reconcile the skipped list on any instances you later upgrade. Instead, you can apply the upgrade then import the update sets containing your changes.

For details on reconciling conflicts, see Process the skipped records list.

**Factors affecting upgrade duration**

Various factors affect how long the system takes to perform an upgrade. The Upgrade Monitor on non-production instance can help you understand those factors and estimate how long the upgrade to your production instance takes.

Many factors can affect the duration of the upgrade process:

• The number of records in the database
• The number of customizations in the database
• The number of nodes in the instance
• The size of tables in the instance that require a schema-change in the instance
• The number of fix scripts required and the size of the tables those fix scripts manipulate

Upgrading a non-production instance can help you estimate how long the upgrade takes on production, but differences between the instances can significantly affect the duration:

• When you cloned the production instance to the non-production instance, you may have clone-excluded some tables. This reduces the size of the database and makes the non-production instance upgrade faster than the production instance.
• The production instance may have more memory and processing power.
• The production instance may have more nodes than the non-production instance.
After upgrading the first non-production instance, examine the Upgrade Summary Report for data to help estimate the impact of these factors.

**Upgrade Monitor schedule states**

When an upgrade is scheduled, the Upgrade Monitor displays information about the next scheduled upgrade. It displays the date and time when the next scheduled upgrade will start. If there is no upgrade scheduled, the Upgrade Monitor displays **Status: No upgrade detected.**

**No upgrade scheduled**

There is no upgrade that has been scheduled currently.

You can also schedule an upgrade by clicking **Schedule upgrade.** To check for an immediately available upgrade, click **Check for upgrade.** It also shows the current version of your upgrade and the date it was upgraded on.
Upgrade scheduled

There is an upgrade that has been scheduled to start at a given time.

You can also reschedule the upgrade by clicking **Reschedule upgrade**. To check for an immediately available upgrade, click **Check for upgrade**. By clicking either **Reschedule upgrade** or **Schedule upgrade**, you will be directed to HI Upgrade Wizard.

Upgrade monitor with issue detected

If one or both of the triggers for upgrading the system ('Check distribution for possible upgrade' and 'Check database for possible upgrade') have been customized or are missing, the Upgrade Monitor displays a warning and provides a button for resolving the issues.

**Note:** If your instance is self-hosted (not hosted by ServiceNow) this message may not necessarily indicate a problem. If you have customized or disabled the upgrade job and want to keep that customization or disabled state, do not click the button to fix the upgrade issue.

To resolve the issues with the upgrade jobs, click the link in the message. This action reverts both upgrade triggers ('Check distribution for possible upgrade' and 'Check database for possible upgrade') to their base versions.
Note: 'Upgrade' job has been renamed to 'Check distribution for possible upgrade' starting Paris. 'Check Upgrade Script' job has been renamed to 'Check database for possible upgrade' starting Paris.

Upgrade History module

The Upgrade History module tracks every upgrade made to an instance. You can also view the complete report of an old upgrade or a recently completed upgrade version using this module.

To view an upgrade history record, navigate to Upgrade Center > Upgrade History and select an upgrade from the list. On selecting an upgrade from the list, the System Upgrades form appears.

System Upgrades form details

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From</td>
<td>Name of the previous .war file (version).</td>
</tr>
<tr>
<td>To</td>
<td>Name of the applied .war file (version).</td>
</tr>
<tr>
<td>Upgrade started</td>
<td>Time stamp when the upgrade process began.</td>
</tr>
<tr>
<td>Upgrade finished</td>
<td>Time stamp when the upgrade process was completed.</td>
</tr>
</tbody>
</table>

Upgrade History Details form section

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Changes skipped</td>
<td>Total number of records that are different from the previous upgrade and the upgrade component was not applied, mostly due to customization.</td>
</tr>
<tr>
<td>Changes applied</td>
<td>Total number of changes that are applied as a part of this upgrade. Changes applied is sum of updated and different records, added to the number of deleted records (where the value of changed is true) added to the number of inserted records (where the value of changed is true).</td>
</tr>
<tr>
<td>Changes processed</td>
<td>Total number of records that were processed as a part of this upgrade. Changes processed is the sum of Changes skipped and Changes applied.</td>
</tr>
<tr>
<td>Copies to review</td>
<td>Total number of copied records to review whose base records have been upgraded.</td>
</tr>
</tbody>
</table>

Click Skipped Record VTB related link to view and manage skipped records over VTB. See Skipped Records visual task board (VTB) for more information.

Click View Upgrade Summary Report related link to view the summary of an older upgrade over Upgrade Monitor module.

See Review skipped records using related lists for more information about related lists.
Previewing an upgrade

Use the Upgrade Preview module to have an insight about the experience of an upgrade prior to the actual upgrade. You can explore and preview upgrades to different ServiceNow release versions and see how your instance might be impacted with your current configurations.

- Preview predicted changes: Preview the changes that have been predicted to occur after an upgrade.
- Upgrade Preview form: Alternate view of a previewed upgrade.

View previewed upgrade

Use the Upgrade Preview form to have an alternate view of a previewed upgrade.

Role required: admin

1. Navigate to Upgrade Center > Preview module.
2. Select the target version to be previewed.
3. Click Go or Refresh Preview to run the selected preview.
4. Click View preview details on the Previewing version card to view the following related lists.
   - Predicted Skips to Review related list: The Upgrade Preview process informs you about the customizations that are predicted to be skipped during an upgrade. The upgrade preview process the skip files that have been customized. Predicted Skips to Review lists all the skipped files that haven't been reviewed yet.
   - Predicted Skips Reviewed related list: Predicted Skips Reviewed related list displays the records which have previously appeared on the Predicted Skips to Review related list and have been reviewed. When you select a skipped record to review and the Resolution Status has been set to a value other than Not Reviewed, the updated record moves to the Predicted Skips Reviewed related list.
• **Previewed Changes related list**: Previewed Changes related list gives the total number of records that are predicted to change when the upgrade occurs. Total record changes also includes possible predicted skip files known as Predicted skipped records.

See [Previewed changes](#) for more details about the related lists.
<table>
<thead>
<tr>
<th>File Name</th>
<th>Priority</th>
<th>Predicted Disposition</th>
<th>Resolution</th>
<th>Upgrade Preview</th>
<th>Related Record</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>test_1.txt</td>
<td>1</td>
<td>Predicted Skip</td>
<td>Not Reviewed</td>
<td>upgrade-06-26-26up_06-26-26up</td>
<td>Related Test - Related Name</td>
<td>page_01</td>
</tr>
<tr>
<td>test_2.txt</td>
<td>2</td>
<td>Predicted Skip</td>
<td>Not Reviewed</td>
<td>upgrade-06-26-26up_06-26-26up</td>
<td>Related Test - Related Name</td>
<td>page_02</td>
</tr>
</tbody>
</table>

Warning: The file names and paths are placeholders and are not intended to represent actual data or file locations.
<table>
<thead>
<tr>
<th>Field</th>
<th>Input Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source version</td>
<td>Current version of the instance</td>
</tr>
<tr>
<td>Target version</td>
<td>Target version to which the instance is upgraded to be previewed</td>
</tr>
<tr>
<td>Preview status</td>
<td>Status of the preview.</td>
</tr>
<tr>
<td></td>
<td>• Pending</td>
</tr>
<tr>
<td></td>
<td>• In Progress</td>
</tr>
<tr>
<td></td>
<td>• Complete</td>
</tr>
<tr>
<td></td>
<td>• Cancelled</td>
</tr>
<tr>
<td></td>
<td>• Failed</td>
</tr>
<tr>
<td>Preview Started</td>
<td>Date and time on which the preview started</td>
</tr>
<tr>
<td>Preview Finished</td>
<td>Date and time on which the preview completed</td>
</tr>
</tbody>
</table>

**Preview predicted changes**

Use the previewed changes table to view the list of total records that are predicted to change when the upgrade occurs.

**Preview skipped list prediction**

The **Total record changes** also includes records that are predicted to be skipped due to various reasons. The most common reason is due to customization. The reason an upgrade skips customizations is to avoid overwriting your customizations. Upgrade Preview attempts to predict which records will be skipped when the actual upgrade occurs. It predicts skips due to customizations, and some of the other more complex scenarios as well. It is possible to use Upgrade Preview to address these predicted customization skips before the upgrade occurs, which can prevent that skip from happening.

Click **View preview details** link on the **Previewing version** card. The Upgrade Preview form appears along with the following related lists details.

**Related lists details**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File name</td>
<td>Record that has been flagged for reconciliation.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Predicted Disposition | Action predicted to be performed on this file during the selected upgrade:  
  • Predicted Insert: The system is predicted to insert a new record.  
  • Predicted Update: The system is predicted to update this record.  
  • Reverted: This record was reverted to the base version, and won’t be skipped on the next upgrade.  
  • Predicted Skip: The system won’t change this record in order to preserve customizations.  
  • Predicted Skip (Manual Merge): The system won’t change this record because updating it requires manual intervention.  
  • Predicted Skip (Apply Once): The system is predicted to skip this record because it had already applied an update from an xml file in the apply once folder. |
| Priority           | Priority that has been assigned to resolve the conflict. Values range from one to five, with one representing the highest priority.  
  **Note:** ServiceNow prioritizes the skipped records based on the importance of the file types. The prioritization is done as follows:  
  • Priority 1 (highest priority): UI pages, UI macros, and more  
  • Priority 2: Business Rules, Security ACLs, and more  
  • Priority 3: Reports and more  
  • Priority 4: Form Sections, Choice Sets, and more  
  • Priority 5 (lowest priority): other |
| Resolution         | Ways to resolve a conflict.  
  • **Not reviewed:** Conflicted files that have not been reviewed yet  
  • **Reviewed:** Reviewed but no action has been taken yet  
  • **Review not needed:** Review of the skipped files are not required  
  • **Reviewed and Retained:** Left customizations in place without update from upgrade  
  • **Reviewed and Reverted:** Customizations discarded, record updated according to the upgrade version |
| Plugin             | Plugin containing the record |
| Related record     | Record that the changelist entry applies to |
Scheduling and monitoring an upgrade

Use the Upgrade Monitor module to schedule and monitor the status of an ongoing upgrade in your instance. You can also view the upgrade summary and the list of records causing conflicts in your instance once the upgrade is complete.

- Monitoring an upgrade: Monitor the progress of an ongoing upgrade in your instance
- Process the skipped records list: Resolve the differences between the upgraded and customized versions of a record by processing the skipped records list
- Resolve conflicts of a record: Resolve conflicts between your customized record and the changes associated with the upgrade

Monitor an upgrade to an instance

Monitor the progress of an ongoing upgrade in an instance with the Upgrade Monitor. When the upgrade is done, you can view a summary of the results on the Upgrade Summary Report.

Role required: admin

1. Navigate to Upgrade Center > Upgrade Monitor.

   ![Note](image)
   
   **Note:** If an upgrade is in progress, the user is automatically directed to Upgrade Center > Upgrade Monitor page.

2. Monitor the progress of the upgrade.

   When the system finishes the upgrade, it displays the Complete upgrade summary report.

   From the Upgrade Summary Report, resolve any conflicts that prevented the system from upgrading records.
Upgrade Progress

When an upgrade is underway, Upgrade Progress displays progress bars and other information to help monitor the process.
## Upgrade Progress details

<table>
<thead>
<tr>
<th>Field</th>
<th>Input Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current version</td>
<td>Current version of the instance</td>
</tr>
<tr>
<td>Target version</td>
<td>Target upgrade version of the instance</td>
</tr>
<tr>
<td>Upgrade Progress</td>
<td>A progress bar depicting where the upgrade is in the overall process. The length of a section in the bar does not indicate the relative duration of that process.</td>
</tr>
<tr>
<td>Upgrade Progress: Upgrading Platform</td>
<td>The system is applying upgrades to elements that form the foundation of the platform.</td>
</tr>
<tr>
<td>Upgrade Progress: Updating Schema</td>
<td>The system is scanning the plugins to create a list of tables that require upgrading. This prevents the system from upgrading the same table multiple times.</td>
</tr>
<tr>
<td>Upgrade Progress: Loading Plugins</td>
<td>The system is loading both core and optional plugins. Some features require more than one plugin, so the number of plugins listed may not match the number of optional features installed.</td>
</tr>
<tr>
<td>Upgrade Progress: Completing</td>
<td>The system is upgrading components that need to be completed after the previous three stages are done.</td>
</tr>
<tr>
<td>Details</td>
<td>Shows the current activity, a progress bar for the current activity, and the file currently being updated.</td>
</tr>
<tr>
<td>Node Upgrades</td>
<td>The color of the icons represents the status of each node during this upgrade: Pending, Running, Successful, Failed, or Down.</td>
</tr>
<tr>
<td>Node</td>
<td>The selected node indicated by the arrow. To change the selection, position the mouse cursor over the icon for the node to select.</td>
</tr>
<tr>
<td>Running time</td>
<td>How long the selected node (indicated by the arrow) has been running. If the selected node is offline, this value stops updating and shows how long a node was online before going offline.</td>
</tr>
<tr>
<td>Version</td>
<td>The current build for the selected node (indicated by the arrow).</td>
</tr>
<tr>
<td>Successful upgrade</td>
<td>When the selected node is online, shows how long the node has been online. If the selected node is offline, shows how long the node has been offline.</td>
</tr>
</tbody>
</table>
# Upgrade Summary Report

The Upgrade Summary report summarizes the actions taken, provides tools to resolve conflicts between customizations and changes that are part of the upgrade, and provides information to help estimate time for upgrades to other instances.

## Completed upgrade summary report

<table>
<thead>
<tr>
<th>Upgraded version</th>
<th>Upgrade duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paris Patch 1</td>
<td>25 Minutes</td>
</tr>
</tbody>
</table>

**Previous version:** Orlando Patch 1

This version is at End-of-Life. Learn more

---

## Find out what's new and changed in Paris Patch 1

Based on your release version, we've provided a list of fixed problems that may be relevant to you. You can also visit the ServiceNow product documentation site to generate personalized release notes, or you can review a list of open known errors on the Known Error Portal.

- View fixed problems in your upgrade
- Generate personalized release notes
- Visit the Known Error Portal
### Upgrade Summary details

<table>
<thead>
<tr>
<th>Field</th>
<th>Input Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgraded version</td>
<td>Version to which the instance has been upgraded</td>
</tr>
<tr>
<td>Upgrade duration</td>
<td>Total time taken to make the upgrade</td>
</tr>
<tr>
<td>Find out what's new and changed</td>
<td>Links to view the new and changed features in the current upgrade version. The following three links show up.</td>
</tr>
<tr>
<td></td>
<td>• Problem fixes: Fixes that have been made since the last upgrade version</td>
</tr>
<tr>
<td></td>
<td>• Personalized release notes: Release notes summary for the previewed version</td>
</tr>
<tr>
<td></td>
<td>• Known error articles: Errors that have been identified but not yet resolved</td>
</tr>
</tbody>
</table>
Skipped Records

Skipped Records from upgrade to Paris Patch 1

When you upgrade to a newer release version, the upgrade can include new features and bug fixes. If customizations are detected during the upgrade, those files are skipped to avoid conflicts. After your upgrade is complete, review these skipped records to decide which version of the files you’d like to keep.

Total record changes

3644 changes

Skipped records

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>62</td>
</tr>
<tr>
<td>To review</td>
<td>58</td>
</tr>
<tr>
<td>Reviewed</td>
<td>4</td>
</tr>
</tbody>
</table>

Skipped records by priority

- Priority 5: 55 (88.7%)
- 10%

Skipped records by product

- Other
- IT Service Manager
- [empty]
- Now Platform

Skipped records code changed/code unchanged

- Code unchanged
- Unable to determine
## Skipped Records details

<table>
<thead>
<tr>
<th>Field</th>
<th>Input Value</th>
</tr>
</thead>
</table>
| Total record changes         | Total number of records that have changed since the previous upgrade version  
|                               | • **Review changes**: List of records that have changed can be reviewed. See *System Upgrade form* for more details.                       |
| Skipped records              | Skipped records to prevent your customizations from being overwritten. If customizations are found in some records during the upgrade, those records are skipped.  
|                               | As an admin, you can resolve each update that was skipped due to a customization. To resolve a skipped update, you can review the reason for each skipped record and then either retain the customization or revert the customization to the base system. If you choose to revert some of the customizations to the base version, those records are sent through the upgrade without getting skipped.  
|                               | • **Total**: Total skipped records  
|                               | • **To review**: Total skipped records that are yet to be reviewed  
|                               | • **Reviewed**: Total skipped records that have been reviewed                                                                                      |
| Skipped records by priority  | ServiceNow prioritizes the skipped records based on the importance of the file types. The prioritization is done as follows:  
|                               | • Priority 1 (highest priority): UI pages, UI macros, and more  
|                               | • Priority 2: Business Rules, Security ACLs, and more  
|                               | • Priority 3: Reports and more  
|                               | • Priority 4: Form Sections, Choice Sets, and more  
|                               | • Priority 5 (lowest priority): other                                                                                                         |
| Skipped records by product   | Skipped records are sorted by product names                                                                                                                                 |
| Skipped records code changed/code unchanged | Skipped records are sorted depending on if there are changes in the code or not. |

**Note:** You can click **Skipped Record VTB** to view the resolution status of the current upgrade with skipped records using the visual task board (VTB) view. See *Skipped Records visual task board (VTB)* for more information.
Node Upgrades

The Node Upgrades section shows the status of the upgrade for each node in the instance. The color of the icon denotes the status, as illustrated by the legend (key) and to the right of the node icons. To see details about a node, position the cursor above the icon for that node. An arrow points to the node selected, and the information below the icons pertains to that node.

Schema Changes to Clone-excluded Tables

The Schema Changes to Clone-excluded Tables section shows a list of tables affected by the upgrade that were clone-excluded when you cloned the production instance to this instance. Because clone-excluded tables are empty, upgrading them takes less time than upgrading those same tables on the production instance. To estimate how much longer the production upgrade takes, note the size of the clone-excluded tables on the production instance.
# Top 10 Fix Scripts by Duration

The Top 10 Fix Scripts by Duration helps you understand which fix scripts required the most time.

<table>
<thead>
<tr>
<th>Duration</th>
<th>Name/Description</th>
<th>Duration</th>
<th>Name/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Second</td>
<td>fix_outage_number.xml</td>
<td>0 Seconds</td>
<td>init.vnc.xml</td>
</tr>
<tr>
<td></td>
<td>Conditionally loads outage number plugin only if the customer does not already have a custom prefix</td>
<td></td>
<td>Fix script on upgrade to populate semaphore sets</td>
</tr>
<tr>
<td>0 Seconds</td>
<td>fix_enable_custom_plugin_on_upgrade.xml</td>
<td>0 Seconds</td>
<td>fix_asm.xml_metric_types.xml</td>
</tr>
<tr>
<td></td>
<td>For Social QA upgrade customers Social QA UI plugin will be activated by default in case we want to ship any Critical UI fixes</td>
<td></td>
<td>sys_script_fix_05412af7f8010556265339a4767ld.xml</td>
</tr>
<tr>
<td>0 Seconds</td>
<td>fix_business_calendar_open_schema.xml</td>
<td>0 Seconds</td>
<td>sys_script_fix_9632a0f0104c04c0c00010064339aa7276754d.xml</td>
</tr>
<tr>
<td></td>
<td>Correct the start and end columns to_datetime for business_calendar_open_schema</td>
<td></td>
<td>sys_script_fix_8898bf3d94c0001003c00010646339a7276754d.xml</td>
</tr>
<tr>
<td>0 Seconds</td>
<td>fix_sys_hub_flow_base_description.xml</td>
<td>0 Seconds</td>
<td>sys_script_fix_8898bf3d94c0001003c00010646339a7276754d.xml</td>
</tr>
<tr>
<td></td>
<td>Fix job for setting the mandatory attribute of description field to false on sys_hub_flow_base_table</td>
<td></td>
<td>sys_script_fix_8898bf3d94c0001003c00010646339a7276754d.xml</td>
</tr>
<tr>
<td>0 Seconds</td>
<td>sys_script_fix_8898bf3d94c0001003c00010646339a7276754d.xml</td>
<td>0 Seconds</td>
<td>sys_script_fix_8898bf3d94c0001003c00010646339a7276754d.xml</td>
</tr>
</tbody>
</table>

View all fix script durations
## Top 10 Schema Changes by Duration

<table>
<thead>
<tr>
<th>Duration</th>
<th>Table Name</th>
<th>Alter Type(s)</th>
<th>Element Names</th>
<th>Row Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 Seconds</td>
<td>sys_upgrade_history_log</td>
<td>add_columns</td>
<td>claim_status</td>
<td>64473</td>
</tr>
<tr>
<td>5 Seconds</td>
<td>sys_upgrade_history_log</td>
<td>batch_alter</td>
<td>sys_upgrade_history_log</td>
<td>65067</td>
</tr>
<tr>
<td>1 Second</td>
<td>sys_cache_flush</td>
<td>batch_alter</td>
<td>sys_cache_flush</td>
<td>429284</td>
</tr>
<tr>
<td>0 Seconds</td>
<td>sys_xce_form_header</td>
<td>batch_alter</td>
<td>sys_xce_form_header</td>
<td>342</td>
</tr>
<tr>
<td>0 Seconds</td>
<td>sys_cluster_state</td>
<td>batch_alter</td>
<td>sys_cluster_state</td>
<td>2</td>
</tr>
<tr>
<td>0 Seconds</td>
<td>upgrade_center_metadata</td>
<td>create_table</td>
<td>upgrade_center_metadata</td>
<td>0</td>
</tr>
<tr>
<td>0 Seconds</td>
<td>sys_declarative_action_group</td>
<td>batch_alter</td>
<td>sys_declarative_action_group</td>
<td>1</td>
</tr>
<tr>
<td>0 Seconds</td>
<td>pa_breakdowns</td>
<td>batch_alter</td>
<td>pa_breakdowns</td>
<td>31</td>
</tr>
<tr>
<td>0 Seconds</td>
<td>ces_table_config</td>
<td>batch_alter</td>
<td>ces_table_config</td>
<td>9</td>
</tr>
<tr>
<td>0 Seconds</td>
<td>sys_sg_xl_parameter</td>
<td>batch_alter</td>
<td>sys_sg_xl_parameter</td>
<td>17</td>
</tr>
</tbody>
</table>

View all schema change durations

The Top 10 Schema Changes by Duration helps you understand which schema changes required the most time.

## Top 10 Plugins by Duration

The Top 10 Plugins by Duration helps you see the plugins that required the most time. Click **View all plugin duration** to see the System Upgrade Metrics list filtered by current sys upgrade history log and sorted by duration. See View loaded files for a plugin for more information.

**View loaded files for a plugin**

Get a related list view of all the files loaded for a plugin by clicking **View all plugin duration**.

Role required: admin

1. Navigate to **Upgrade Center > Upgrade Monitor**.
   When the system finishes the upgrade, it displays the Upgrade Summary Report.
2. Scroll down to **Top 10 Plugins by Duration**.
3. Click **View all plugin duration**.
   The System Upgrade Metrics list of all the plugins and their durations shows up.
4. Click one of the plugins from the list to open the **System Upgrade Metrics** form view of that plugin. The Plugin Files related list of all the loaded files for that plugin is displayed.

<table>
<thead>
<tr>
<th>File Name</th>
<th>Disposition</th>
<th>Load Duration</th>
<th>Claim Status</th>
<th>Priority</th>
<th>Resolution</th>
<th>Comment</th>
<th>Target Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>credb_business_rule_exclusions_importer_...</td>
<td>Updated</td>
<td>295 ms</td>
<td>Priority 5</td>
<td>credb_ci_variable_definition_disk</td>
<td>Bus Rule</td>
<td>Enc List</td>
<td></td>
</tr>
<tr>
<td>ins_security_ad_rule_4eb6e7f7b11f3202_...</td>
<td>Unchanged</td>
<td>0 ms</td>
<td>Priority 5</td>
<td>JRL_admin</td>
<td>Acc</td>
<td>RL</td>
<td></td>
</tr>
<tr>
<td>ins_security_ad_rule_4eb6e7f7b11f3202_...</td>
<td>Unchanged</td>
<td>0 ms</td>
<td>Priority 5</td>
<td>JRL_admin</td>
<td>Acc</td>
<td>RL</td>
<td></td>
</tr>
<tr>
<td>ins_security_ad_rule_4eb6e7f7b11f3202_...</td>
<td>Unchanged</td>
<td>0 ms</td>
<td>Priority 5</td>
<td>get_metadata_rule_types.kil</td>
<td>Acc</td>
<td>RL</td>
<td></td>
</tr>
<tr>
<td>ins_security_ad_rule_4eb6e7f7b11f3202_...</td>
<td>Unchanged</td>
<td>0 ms</td>
<td>Priority 5</td>
<td>credb_rc_type_definitions.kil</td>
<td>Acc</td>
<td>RL</td>
<td></td>
</tr>
<tr>
<td>ins_security_ad_rule_4eb6e7f7b11f3202_...</td>
<td>Unchanged</td>
<td>0 ms</td>
<td>Priority 5</td>
<td>regbank_xi_icona_kil_admin</td>
<td>Acc</td>
<td>RL</td>
<td></td>
</tr>
<tr>
<td>ins_security_ad_rule_4eb6e7f7b11f3202_...</td>
<td>Unchanged</td>
<td>0 ms</td>
<td>Priority 5</td>
<td>/newcondi/querybuilder/credb_query_builder...</td>
<td>Acc</td>
<td>RL</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** The total plugin load duration is not the sum of the load duration of all the loaded files for that plugin.
Process the skipped records list

Process the skipped records list to resolve the differences between the upgraded and customized versions of a record. If you have customized or altered a record affected by this upgrade, such as a business rule or script, the upgrade generates a skip log record.

Role required: admin

Review the changes you made to baseline records, such as business rules and scripts, that appear on the skipped records list and revert to the baseline version if appropriate. Post-upgrade, thoroughly test all changes you made to these records.

1. Navigate to Upgrade Center > Upgrade Monitor.
   
   If the upgrade is still in progress, the system displays the Upgrade Progress screen. When the upgrade finishes, the system displays the Upgrade Summary Report.

2. After the system displays the Upgrade Summary Report, click the Review changes link in the Skipped box.
   
   The system displays the System Upgrades form.


4. Click the row for the first record you want to reconcile.
   
   The system displays the Upgrade details form for that record.

5. Evaluate how you want to resolve the conflict for this record and take the appropriate action:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retain the customized record as is and do not update it</td>
<td>After reviewing the changes, set Resolution Status to Reviewed and Retained. The record moves from the Skipped Changes to Review to Skipped Changes Reviewed related list. See Review skipped records using related lists.</td>
</tr>
</tbody>
</table>
   | Retain the customization by merging changes from the updated object | a. Click Resolve Conflicts to navigate to the Resolve Conflicts form.  
   b. Review the differences.  
   c. To merge a field:  
   • Click the right-arrow button for the field.  
   • Click a text box to view and edit the detailed differences.  
   • When you have merged all appropriate fields, click Merge.  
   After merging the customization changes:  
   • The Disposition changes from Skipped to Merged.  
   • The Resolution Status changes to Reviewed and Merged.  
   • The record moves from the Skipped Changes to Review to the Skipped Changes Reviewed related list. |
<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discard the customization and update the record to match the base system for this upgrade</td>
<td>After reviewing the changes, click <strong>Revert to Base System</strong>. &lt;br&gt;• The <strong>Disposition</strong> changes from <strong>Skipped</strong> to <strong>Reverted</strong>. &lt;br&gt;• The <strong>Resolution Status</strong> changes to <strong>Reviewed and Reverted</strong>. &lt;br&gt;• The system creates a Customer Update record. &lt;br&gt;• The record moves from the Skipped Changes to Review to the Skipped Changes Reviewed related list.</td>
</tr>
<tr>
<td>Review the skip and perform no action on the object</td>
<td>After reviewing the changes, set <strong>Resolution Status</strong> to <strong>Reviewed</strong>. The record moves from the Skipped Changes to Review to the Skipped Changes Reviewed related list.</td>
</tr>
<tr>
<td>Leave on the skipped list for a later decision, and note that you have not reviewed the record</td>
<td>From the <strong>Resolution</strong> list, choose <strong>Not Reviewed</strong> to defer the decision on how to handle this conflict. The record stays on the Skipped Changes to Review related list.</td>
</tr>
</tbody>
</table>

**Note:** The system tracks changes to records in an update set so you can apply these changes to another instance later. However, the system does not migrate the upgrade details records from one instance to the next. These records apply to a specific upgrade of a specific instance. If you want to preserve the Comments, Resolutions, or other information from the skipped list, export it from this instance.

6. In the **Comment** field, write the reasons for making your decision and other information you want to document.

7. Click **Update**.  
   Post-upgrade, thoroughly test all changes you made to the records on the skipped record list.
System Upgrade form

When an upgrade is complete, the System Upgrades form displays key statistics about the upgrade and a related list of skipped records (the skipped list).
## System Upgrade details

<table>
<thead>
<tr>
<th>Field</th>
<th>Input Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>From</td>
<td>Version of the instance before upgrading.</td>
</tr>
<tr>
<td>To</td>
<td>Version of the instance after upgrading.</td>
</tr>
<tr>
<td>Upgrade started</td>
<td>Time of the start of the upgrade.</td>
</tr>
<tr>
<td>Upgrade finished</td>
<td>Time at which the upgrade completed.</td>
</tr>
<tr>
<td>Changes skipped</td>
<td>Total number of records that are different from the previous upgrade and the upgrade component was not applied, mostly due to customization.</td>
</tr>
<tr>
<td>Changes applied</td>
<td>Total number of changes that are applied as a part of this upgrade.</td>
</tr>
<tr>
<td>Changes processed</td>
<td>Total number of records that were processed as a part of this upgrade.</td>
</tr>
<tr>
<td>Copies to review</td>
<td>Total number of copied records to review whose base records have been upgraded</td>
</tr>
</tbody>
</table>

## Resolve conflicts for an individual record

Reconcile differences between your customized record and the changes associated with the upgrade.

Role required: admin

1. From the Upgrade Details form for the record you are reconciling, click **Resolve Conflicts**.

   The system displays the Resolve Conflicts form, which highlights differences between the two versions of the record. The form displays information about the base system record on the left and the customized record on the right.

   **Note:** The system creates a new customer update record when you click **Resolve Conflicts**.

2. Compare the base system with the customized record for each field on this form. For non-script fields, edit the customized record on the right-hand side to include what you want from the base system and the customization.

3. If this record contains a script, check it for conflicts and resolve.
   a. Click inside the Script field.

      The system displays the Resolve Conflicts - Script form highlighting areas where the two versions of the script differ.

   b. Edit the right-hand side so that the script contains whichever content you want. To move a block of code from the left to right side, click the small arrows corresponding to that block in the middle column.

   c. Click **OK**.

   The system returns to the Resolve Conflicts form.
4. To save your changes to the record, click **Save Merge**.

   The system sets the **Resolution** for this record to **Reviewed and Merged**.
Upgrade details form

From the Upgrade Details form, you can review an individual record affected by the upgrade and reconcile conflicts between the upgrade and customizations.
Use the following fields to track your progress in reviewing skipped records:
- Priority is based on the elements contained within the record. For example, a Business Rule has a higher priority than a UI Page because it contains script, SQL, and HTML fields.
- Use Resolution Status to keep track of whether the skipped record was reviewed and ignored, retained in its customized form, or reverted to the base system version.
- You can add Comments to a record to keep a log of your thoughts and actions.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>script_H/71226/M0122200300004/9171623105C</td>
</tr>
<tr>
<td>Priority</td>
<td>Priority 2</td>
</tr>
<tr>
<td>Comment</td>
<td></td>
</tr>
<tr>
<td>Hasresolution</td>
<td>Not Reviewed</td>
</tr>
<tr>
<td>Disposition</td>
<td>Skipped</td>
</tr>
<tr>
<td>Target Name</td>
<td>Assign to front stock</td>
</tr>
<tr>
<td>Type</td>
<td>Business Rule</td>
</tr>
<tr>
<td>Update set</td>
<td></td>
</tr>
<tr>
<td>Table</td>
<td>scripts.product_catalog</td>
</tr>
<tr>
<td>Notes</td>
<td></td>
</tr>
</tbody>
</table>

The Resolve Conflict page displays a side-by-side comparison of the base system record and the corresponding customized record. Use the built-in diff editor to resolve conflicts in multi-line text fields.

Related Links
- Show Related Record
- Upgrade History Tasks
- Search Number
- Number
- Short description
- Priority
- Assigned to
- Assign from Stock (Business Rule from Now Platform)

© 2021 ServiceNow, Inc. All rights reserved.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
## Upgrade Details form details

<table>
<thead>
<tr>
<th>Field</th>
<th>Input value</th>
</tr>
</thead>
<tbody>
<tr>
<td>File name</td>
<td>The record the system has flagged as needing to be reconciled.</td>
</tr>
<tr>
<td>Priority</td>
<td>The priority the system has assigned to resolving this conflict. Values range from one to five, with one representing the highest priority.</td>
</tr>
<tr>
<td>Comment</td>
<td>Comments to document your decisions about reconciling this record.</td>
</tr>
<tr>
<td>Resolution</td>
<td>How you elected to resolve this conflict:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Not reviewed</strong>: Not yet reviewed</td>
</tr>
<tr>
<td></td>
<td>• <strong>Reviewed</strong>: Reviewed but no action yet taken</td>
</tr>
<tr>
<td></td>
<td>• <strong>Reviewed and Merged</strong>: Made changes to the record to reconcile the customized and upgraded versions</td>
</tr>
<tr>
<td></td>
<td>• <strong>Reviewed and Retained</strong>: Left customizations in place without update from upgrade</td>
</tr>
<tr>
<td></td>
<td>• <strong>Reviewed and Reverted</strong>: Customizations discarded, record updated according to upgrade</td>
</tr>
<tr>
<td></td>
<td>For more information, see Process the skipped records list.</td>
</tr>
<tr>
<td>Disposition</td>
<td>Action performed on this file during the selected upgrade:</td>
</tr>
<tr>
<td></td>
<td>• Inserted: The system inserted a new record</td>
</tr>
<tr>
<td></td>
<td>• Updated: The system updated the record</td>
</tr>
<tr>
<td></td>
<td>• Deleted: The system deleted the record</td>
</tr>
<tr>
<td></td>
<td>• Skipped: The system did not change this record in order to preserve customizations</td>
</tr>
<tr>
<td></td>
<td>• Reverted: This record was reverted to the base version</td>
</tr>
<tr>
<td></td>
<td>• Table not found: The system could not find the table that contains this record</td>
</tr>
<tr>
<td></td>
<td>• Unchanged: The system did not change this record because the baseline component has not changed since the last release</td>
</tr>
<tr>
<td></td>
<td>• Skipped Manual Merge: The system did not change this record because updating it requires manual intervention</td>
</tr>
<tr>
<td></td>
<td>• Skipped Apply Once: The system skipped this record because it had already applied an update from an xml file in the apply once folder</td>
</tr>
<tr>
<td></td>
<td>• Not Latest: The system applied a change, but this change was overwritten later during the same upgrade.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of the record, for example <em>Script include</em>.</td>
</tr>
<tr>
<td>Target name</td>
<td>Name of the skipped record, if applicable.</td>
</tr>
<tr>
<td>Update set</td>
<td>Unused.</td>
</tr>
<tr>
<td>Plugin</td>
<td>The plugin containing this record.</td>
</tr>
<tr>
<td>Table</td>
<td>The table containing this record.</td>
</tr>
</tbody>
</table>
**Resolve Conflicts form**

The Resolve Conflicts form you compare to the base system version with the customized version of a record and reconcile the differences.
### Base System vs Customized

<table>
<thead>
<tr>
<th>Field</th>
<th>Base System</th>
<th>Customized</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action</strong></td>
<td>INSERT, UPDATE</td>
<td>INSERT, UPDATE</td>
</tr>
<tr>
<td><strong>Alert action</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Accessible from</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Delete</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Insert</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Query</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Update</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Active</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Add message</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Advanced</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Update reference fields</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Client callable</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Table</strong></td>
<td>RequestedItem [ac_item]</td>
<td>RequestedItem [ac_item]</td>
</tr>
<tr>
<td><strong>Condition</strong></td>
<td>current_configuration, itemchanged &amp;&amp; current_configuration, itemw()</td>
<td>current_configuration, itemchanged &amp;&amp; current_configuration, itemw()</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Execute function</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Filter Conditions</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web Services</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Message</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Fields

The fields this form displays depend on the type of record you are reconciling. The left column shows the records fields in the base system, including the proposed changes that are part of the upgrade. The right column shows the fields for your customized record.

Reviewing upgrade history

The Upgrade History module tracks every upgrade made to an instance. You can also view the complete report of an old upgrade or a recently completed upgrade version using this module.

- **Upgrade history related lists:** Use the related lists to resolve, track and review the skipped records in an upgrade
- **Visual task board (VTB) view of skipped records:** Use the VTB view to see the resolution status of any previous upgrade with skipped records

Review skipped records using related lists

Use different related lists to resolve, track and review the skipped records in an upgrade.

Role required: admin

1. Navigate to Upgrade Center > Upgrade History.
   A list of upgrades is displayed.
2. Select an upgrade from the list.
   System Upgrades form is displayed.
3. Select any of the following related lists to review the skipped records.
   - **Skipped Changes to Review related list**
     Resolve the skipped update records by tracking and reviewing them in the Skipped Changes to Review related list. To prevent your customizations from being overwritten during system upgrades, the upgrade process skips (does not apply the update to) objects that have been customized. See Resolve a skipped update and set a resolution status for more information.
   - **Skipped Changes Reviewed related list**
     View the list of the reviewed skipped records in the Skipped Changes Reviewed related list. When you select a skipped record to review and set a Resolution Status to a value other than Not Reviewed, the update record moves from Skipped Changes to Review related list to the Skipped Changes Reviewed related list.
   - **Copies to Review related list**
     Copies to Review lists all the records that need to be reviewed.
   - **Copies Reviewed related list**
     Copies Reviewed lists all the records that have been reviewed.
   - **Customization Unchanged related list**
     Customizations Unchanged lists all records that were skipped (due to a customization), but there have been no changes from the last upgrade. See Revert a customization for more information.
   - **Changes Applied related list**
     Changes Applied lists all changes that were applied in this upgrade.
   - **Claim Outcomes to Review related list**
     During system upgrades, the Claim Status tab displays outcomes to review and resolve.
   - **Upgrade Details related list**
Upgrade Details lists all Upgrade Details records for this upgrade.

**Note:** The Copies to Review and Copies Reviewed related lists are Platform specific related lists.

## Upgrade history related lists details

The following table gives the description of each field in all the related lists within the upgrade history module.

### Related lists details

<table>
<thead>
<tr>
<th>Field</th>
<th>Input Value</th>
</tr>
</thead>
</table>
| File name                  | File name has different description for different related lists  
  • Skipped Changes to Review related list: Name of skipped Upgrade Detail record  
  • Skipped Changes Reviewed related list: Name of the reviewed Upgrade Detail record  
  • Copies to Review related list: Name of the record that needs to be reviewed  
  • Copies Reviewed related list: Name of the record that has been reviewed  
  • Customization Unchanged related list: Name of unchanged sys_upgrade_history_log record. Select it if you want to access Upgrade Details and add comment text, or set a resolution status for it  
  • Changes Applied related list: Current upgrade file name  
  • Claim Outcomes to Review related list: Name of skipped Upgrade Detail record  
  • Upgrade Details related list: Current upgrade file name |

| Disposition                | Action performed on this file during the selected upgrade:  
  • Inserted: The system inserted a new record.  
  • Updated: The system updated this record.  
  • Deleted: The system deleted this record.  
  • Skipped: The system did not change this record in order to preserve customizations.  
  • Reverted: This record was reverted to the base version.  
  • Table not found: The system could not find the table that contains this record.  
  • Unchanged: The system did not change this record because the baseline component has not changed since the last release.  
  • Skipped Manual Merge: The system did not change this record because updating it requires manual intervention.  
  • Skipped Apply Once: The system skipped this record because it had already applied an update from an xml file in the apply once folder.  
  • Not Latest: The system applied a change, but this change was overwritten later during the same upgrade. |
### Revert a customization

To prevent customizations from being overwritten by system upgrades, the upgrade process automatically skips changes to objects that have been customized. You may want to overwrite your customizations when a software upgrade contains a feature that you would like to implement.

**Role required:** admin

To identify customized objects, the system adds a corresponding record in the Customer Updates [sys_update_xml] table. The table maintains the current version information for all objects that have been customized. The upgrade process skips changes to objects that have entries in the table. The upgrade process does not skip objects if only excluded fields have changed.

1. Navigate to **Upgrade Center > Upgrade History**.
2. Select the desired software version.
3. Filter the Upgrade Details related list by **Disposition is Skipped**.
4. Optional: Add another filter condition for **Changed is True** to return only the objects that have changed since the last upgrade.
5. Select the update record to implement.

The **File differences** field displays a side-by-side comparison of the customization and the default version. Deletions are highlighted in red, additions in green, and modifications in yellow.
6. Click **Revert to base system** to overwrite your customized object with the system default version.

   - The Disposition changes from **Skipped** to **Reverted**.
   - After you revert a customization, you have the option to click **Reapply Changes** to reapply your customizations (undo the revert).

**Resolve a skipped update and set a resolution status**

Review the reason for each skipped record to resolve each skipped update after an upgrade.

Role required: admin

You resolve an update by either retaining the customization or by merging or overwriting the customization with the base system update.

**Note:** Objects that are customized and that did not change in the base system since the last upgrade require no action on your part.

When an object is customized, the system adds a corresponding record to the Customer Updates [sys_update_xml] table and then maintains current version information for all customized objects. The upgrade process skips changes to objects that have a current version in the Customer Updates table. When you follow the procedure, you perform one of the following actions:

- Retain a customization with no changes
- Retain a customization by merging changes from the updated object
- Revert a customized object to the updated version (that is, overwrite the customization)
- Review the skip and perform no action on the object

1. Navigate to **Upgrade Center > Upgrade History**.
2. Select the desired software version.
3. In the Skipped Changes to Review related list, select the update record to resolve. See **Review skipped records using related lists**.
4. Review the list of changes. For text fields, you can click in the field to open the Diff/Merge tool. Review the differences. Click a text box to view and edit the detailed differences.
5. Perform one of the following actions. You have the option to add a **Comment** to any record, for example, to explain the action to future reviewers.

  **Skipped Changes to Review related list**

<table>
<thead>
<tr>
<th>Field</th>
<th>Input Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retain the customized record as is and do not update it.</td>
<td>After reviewing the changes, set <strong>Resolution Status</strong> to <strong>Reviewed and Retained</strong>. The record moves from the Skipped Changes to Review to Skipped Changes Reviewed related list.</td>
</tr>
</tbody>
</table>
### Field
Retain the customization by merging changes from the updated object.

### Input Value
- **a.** Click Resolve Conflicts to navigate to the Resolve Conflicts form.
- **b.** Review the differences.
- **c.** To merge a field:
  - Click the right-arrow button for the field.
  - Click a text box to view and edit the detailed differences.
  - When you have merged all appropriate fields, click **Merge**.

After merging the customization changes:
- The Resolution Status changes to Reviewed and Merged.
- The record moves from the Skipped Changes to Review to the Skipped Changes Reviewed related list.

### Field
Discard the customization and update the record to match the base system for this upgrade.

### Input Value
After reviewing the changes, click **Revert to Base System**.
- **Disposition** changes from **Skipped** to **Reverted**.
- **Resolution Status** changes to **Reviewed and Reverted**.
- The system creates a Customer Update record.
- The record moves from the Skipped Changes to Review to the Skipped Changes Reviewed related list.

#### Note:
At any time after you revert a customization, you can click **Reapply Changes** to reapply the customization.

### Field
Review the skip and perform no action on the object.

### Input Value
After reviewing the changes, set **Resolution Status** to **Reviewed**. The record moves from the Skipped Changes to Review to the Skipped Changes Reviewed related list.

### Field
Leave on the skipped list for a later decision, and note that you have not reviewed the record.

### Input Value
From the **Resolution** list, choose **Not Reviewed** to defer the decision on how to handle this conflict. The record stays on the Skipped Changes to Review related list.

6. Click **Update**. Repeat the process to resolve each update record in the list.

Only skipped updates with a **Resolution Status** of **Not Reviewed** or without a resolution set appear in the Skipped Changes to Review related list. Any action you take that changes the **Resolution Status** to a value other than **Not Reviewed** or **--None--** removes the skipped update from list and moves it to the Skipped Changes Reviewed related list.
Skipped Records visual task board (VTB)

View the resolution status of any previous upgrade with skipped records using the visual task board (VTB) view. An upgrade history record is created for each upgrade that is run.

To view the history report navigate to Upgrade Center > Upgrade History. You can then select an upgrade from the list to view the upgrade history details. Click the Skipped Record VTB related link to view and manage the skipped records over VTB.

**Note:** The Skipped Record VTB related link shows up only when there are skipped records for the version upgrade.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Reviewed</td>
<td>Tasks which have not been reviewed</td>
</tr>
<tr>
<td>Reviewed</td>
<td>Tasks which have been reviewed</td>
</tr>
<tr>
<td>Merged</td>
<td>Tasks which have both the old and new changes</td>
</tr>
<tr>
<td>Retained</td>
<td>Tasks which have retained the updates from the latest upgrade</td>
</tr>
<tr>
<td>Reverted</td>
<td>Tasks which have reverted its changes to the base system</td>
</tr>
</tbody>
</table>

The skipped records are prioritized based on the importance of the file types. The prioritization is done as follows:

- Priority 1 (highest priority): UI pages, UI macros, and more
- Priority 2: Business Rules, Security ACLs, and more
- Priority 3: Reports and more
- Priority 4: Form Sections, Choice Sets, and more
- Priority 5 (lowest priority): other
Upgrade History Task form

You can update information about a skipped record task using the Upgrade History Task form.

To make changes on a skipped record task, click a task number link on a task over VTB.

**Upgrade History task form details**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short description</td>
<td>Description about the task</td>
</tr>
</tbody>
</table>
| Priority      | Prioritization of the skipped records based on the importance of the file types. The prioritization is done as follows:  
  • Priority 1 (highest priority): UI pages, UI macros, and more  
  • Priority 2: Business Rules, Security ACLs, and more  
  • Priority 3: Reports and more  
  • Priority 4: Form Sections, Choice Sets, and more  
  • Priority 5 (lowest priority): other |
| Disposition   | Disposition is Skipped since the task board is only for skipped records. The system did not change this record in order to preserve customizations. |
| Type          | Type of file which determines the priority level. |
| State         | State of the files.  
  • Not reviewed: Tasks which have not been reviewed  
  • Reviewed: Tasks which have been reviewed  
  • Merged: Tasks which have both the old and new changes  
  • Retained: Tasks which have retained the updates from the latest upgrade  
  • Reverted: Tasks which have reverted its changes to the base system |
| Work notes    | Notes about the skipped record task |
| Update        | Button to update the skipped record task |
| Resolve Conflicts | Button to resolve conflicts by reviewing the differences |
| Revert to Base System | Button to revert the customizations |
| Delete        | Button to delete the skipped record task |
The Old Resolution Details related list shows the actions taken in the previous upgrade version.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>Task number of the skipped file where some actions were taken in the previous upgrade version.</td>
</tr>
<tr>
<td>Short description</td>
<td>Description about the task</td>
</tr>
<tr>
<td>Disposition</td>
<td>Action performed on this file during previous upgrade</td>
</tr>
</tbody>
</table>
| Priority           | Prioritization of the skipped records based on the importance of the file types. The prioritization is done as follows:  
1. (highest priority): xml content  
2. script or script_plain  
3. html content  
4. sys_ui_form_section, sys_ui_related_list, or sys_choice_set  
5. (lowest priority): other |
| State              | State of the files.  
• Not reviewed: Tasks which have not been reviewed  
• Reviewed: Tasks which have been reviewed  
• Reviewed and Merged: Tasks which have been reviewed and have both the old and new changes  
• Reviewed and Retained: Tasks which have been reviewed and have retained the updates from the latest upgrade  
• Reviewed and Reverted: Tasks which have been reviewed and have reverted its changes to the base system |
| Assigned to        | Name of the assigned user                                                   |
| From               | Past previous version                                                       |
### Update default labels in VTB view

Filter skipped records in the task board of the VTB with the implementation of color-coded labels. You can filter the skipped records by assigning a color to each of the products.

Role required: admin

1. Navigate to **Upgrade Center > Upgrade History**.
2. Select an upgrade from the list.
   The System Upgrades form appears.
3. Click the **Skipped Record VTB** related link to view the resolution status of the skipped records over VTB.

   **Note:** The **Skipped Record VTB** related link shows up only when there are skipped records for the version upgrade.

   The VTB view of the resolution status of the skipped records shows up.

4. Click **Labels** to show the default labels.
   The default labels consist of Include codes, Does not include code and Others categories.

   **Note:** The Include and Does not include codes categories indicate if there is any change in the code of the skipped records. All products fall under Other category of labels. The product labels are assigned with different colors. The tasks get assigned based on the label colors of the products.
5. Optional: If you want to add a label, click **Add Label**.

Enter the name of the label you want to create. You can also change the color of a label by clicking the color circle.

![Labels](image)

**Note:** The new labels and colors are saved only for the current visual task board and don't get rolled over to the next updated board. If you want the new label updates to show up in the next updated board, navigate to **Upgrade Center > Administration > Properties > Upgrade Center VTB Labels**. Set the colors as required and the updated colors start showing up from the next generated board.

Click on a skipped record in the VTB to update the task. See **Upgrade History Task form** for more information.
View import history

View your import history by accessing the **My Application Import History** module.

Role required: admin

1. Navigate to **System Applications** > **My Application Import History**. The list of import history records in your instance shows up.
2. Select one of the imports from the list for more information about that import. The form view of sys_upgrade_history record shows up.

**Note:** To learn more about importing from Source Control, see ServiceNow Studio. Once the importing is done, use the **My Application Import History** module to view the import history.

Quick access to plugins and history records

Reduce the navigating time by directly accessing plugins, application installation history records, and update set commits history records. The filters for the plugins and history records are automatically implemented in the plugins and history records views.

Role required: admin

**Plugins and application installation history records**

1. Navigate to **System Definition** > **Plugin Installation History**.
2. Select any of the plugins or history records to access them directly.

**Update set commit history records**

1. Navigate to **System Update Sets** > **Update Sets to Commit**.
2. Select any of the update sets to directly view the commit history of that update set.

Explore upgrade history log

Reduce processing time by extracting all upgrade related logs into a separate file named database-upgrade_<timestamp>.log. You can also zip the file and attach it to upgrade history.

Role required: admin

When the upgrade starts, the upgrade log messages are written to both the localhost_log file and the database-upgrade_<timestamp>.log file. When the upgrade is done, the database-upgrade_<timestamp>.log file is uploaded to the upgrade history table.

1. Navigate to **System Logs** > **Utilities**.

**Note:** You can implement this step to view the extracted database-upgrade_<timestamp>.log file only after the upgrade is done.
2. Click **Node Log File Download**.
   The database-upgrade_<timestamp>.log file appears in the list of log files.

   **Note:** The localhost_log file consists of all the logs. The database-upgrade_<timestamp>.log file consists of logs only related to the upgrade.

3. Go to **Upgrade Center > Upgrade History**.
   A list of upgrades shows up.

4. Click the required upgrade from the list. You can see database-upgrade_<timestamp>.log file is automatically attached to the upgrade.

   **Note:** The database-upgrade_<timestamp>.log file gets attached only if the glide.db.upgrade.log.save_to_db.enabled property is set to True. By default, the glide.db.upgrade.log.save_to_db.enabled is set to True.

5. Download the zipped database-upgrade_<timestamp>.log file.

   **Note:** The database-upgrade_<timestamp>.log file has been zipped to reduce the download time.

### Administration

The Administration module contains properties for managing .

### Properties

On the properties form, you can set parameters that control how the system executes.

**Upgrade Duration Estimation Properties**

<table>
<thead>
<tr>
<th>Field / Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queries upgrade duration estimate</td>
<td>A non-production instance queries the upgrade duration estimate. If this property is absent, the system uses all remote instance records to query the upgrade duration estimate. You can also copy the sys_id of the remote instance record you wish to query for upgrade duration estimate. The system uses the highest duration from the results.</td>
</tr>
<tr>
<td>glide.upgrade.preview.duration.instance.id</td>
<td></td>
</tr>
</tbody>
</table>

**Upgrade Visual Task Board Properties**

<table>
<thead>
<tr>
<th>Field / Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable an admin or user with admin role to own Upgrade VTB</td>
<td>Upgrade VTB owner must be an admin. If this property is absent, the system uses the first admin user from active admin users list. The active admin users list is sorted by username.</td>
</tr>
<tr>
<td>glide.upgrade.center.task_board.owner</td>
<td></td>
</tr>
<tr>
<td>Field / Element</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable admins or users with admin role to be members of Upgrade VTB glide.upgrade_center.task_board.members</td>
<td>Upgrade VTB members must be an admin. If this property is absent, the system adds all active admin users as members.</td>
</tr>
</tbody>
</table>

**Upgrade Center VTB Labels list**

The Upgrade Center VTB Labels list under Administration module shows all the labels in the Upgrade Visual Task Board (VTB). You can also change the color of the existing labels.

If you want to change the color of an existing label, navigate to **Upgrade Center > Administration > Properties > Upgrade Center VTB Labels**

---

**Note:** If you update the color of an existing label, the change will not be reflected in the current version upgrade related board. The change will be seen only from the next version upgrade.
Index

A

access account
  LDAPS 1701
access control 2090
access controls 2090
ACL 2090
ACLs 2090
  configuration watcher 2117
  execution plan 2118
  using 2119
controlling whether script conditions apply to reference fields 2113
creating ACL rules 2102
debugging 2114
evaluate the admin override at the access level 2114
hasRoles() 2112
mandatory roles 2112
provide access to users 2112
snc_internal 2112
troubleshooting 2116
Activate fiscal calendar 959
activate plugins 14, 14
activated by maint 17
active directory application mode (ADAM)
  access account 1701
  backup 1699
  configuring 1695
  console 1697
  container 1697
  create objects 1698
  delegation 1697
  dependencies 1694
  group objects 1698
  instance 1695
  LDAPS 1699
  LDAPS certificate 1700
  LDAPS connection 1701
  objects 1698
  organizational unit 1697
  permission 1698
  public key fCertificate 1700
  recovery 1699
  redundancy 1699
  security 1694
  testing 1698
  troubleshooting 1698
  user objects 1698
  userproxy objects 1698
Active Directory Federation Services
  creating a SAML logout 1762
  identity provider 1755, 1755, 1757, 1757, 1757, 1762, 1762, 1763
Active Directory, configure SSL access 1706
active transactions
  killing 1894
  viewing 1894
activities list
  customize 564
activity formatter 561
add to a form 563
create 563
e-mail property 566
live feed 563
security 561
activity stream
  max entries 574
ADAM
  ADAM Sync 1701, 1701, 1702, 1703, 1703
  configuration file 1703, 1703
  configuring 1695
  dependencies 1694
  example 1703
  instance 1695
  security 1694
  set up 1702
  user accounts 1701
add
  field  table 716
add role
  table 716
adding
  new department 1581
  suggestion fields 710
ADFS 1755, 1755, 1757, 1757, 1762, 1762, 1763
  See also Active Directory Federation Services
administer
  table administration
    unique record identifier 1304
    unique record identifier 1304
Advanced Reporting
  database views 467, 468, 469, 475, 476, 476, 477, 479, 479
  metric definition support 1851, 1851, 1852, 1853
AES 128
  configure 2306
  encryption key 2306
AES 256
  configure 2310
  encryption key 2310
Allow IP Addresses 2362
altiris integration 1561
annotate
  forms 553
  annotate forms 553
application development 1527
application quotas 1935
  property 1936
  rules 1936
Application Usage Overview 1615
applications
  create a custom table 355, 360
apply ACLs
  AJAXGlideRecord 2113

© 2021 ServiceNow, Inc. All rights reserved.
approval summarizer

attachment

configuring

icon 558

disabling

table 557, 1101

file size

limiting 556

file types 1099

icon

configuring 558

table

disabling 557, 1101

viewing 553

attachments

administering 553

restrict file extensions 556

hide attachment [view] link 558

audit 2574

audit roles 2111

audit roles table

sys_audit_role 1612

auditing

reference fields 2427

authentication 1618

multifactor 1816, 1820

activating 1818, 1822, 1824

configuring 1819

disabling for a role 1821

disabling for a user 1820

disabling on user table 1825

disabling on your user profile 1825

logging on 1823

requiring for a role 1821

requiring for a user 1820

two-factor 1816, 1820

auto-upgrade 2348

auto-upgrader 2348

Automatic cloning 1531

B

backup

active directory application mode (ADAM) 1699

ADAM 1699

Base system 261

Base System Roles

special administravive roles 1602

breadcrumbs

restricting 501

suppressing 501

Breadcrumbs

restricting 498

browser support

list v3 519

C

calculated price fields 796

calendar

schedule 977

Calendars

creating 974, 976

certificate

certificate authority (CA) 2158

configure 2306

generate with keytool 2158

https 2306

trusted server 2160

upload 2159

certificates 2156

LDAP client 2158

mutual authentication 2158

child record 576

choice list

time zone 939

choice list state field 613

CI changes 2424

CI relationships and history 2427

Client Transaction Timings 1022, 1024, 1024, 2431

Clone status 1533

cmdb ci changes 2424

certificate authority (CA) 2158

certificates 2156

LDAP client 2158

mutual authentication 2158

computer telephony integration 1566

connection

count widget

add 621

configure audits 2574

configure group types

assignment groups 1594

configure transaction quota rule 1932

configuring

attachment

icon 558

icon

attachment 558

suggested text

journal fields 712

string fields 711

connection

LDAPS 1701

testing 1701

connection test module

creating 1926

container

ADAM 1697

create 1697

context menus

action script 518

create 513

dynamic actions script 518

onshow script 519

context ranking 506

definition, creating 507

list, ranking 508

plug-in, activate 506

scrum ranking 511

sort order, apply 511

update sets 507
contextual search 1229
contextual security 2090, 2107, 2108
configuring 492
Contextual Security: Role Management V2 2109
Contextual Security: Role Management V2 REST API 2109
Contextual Security: Role Management V2 2111
conversions 2577
Core configuration 13
Core Configuration
  List Administration 481
  overview 822
  Platform Performance 1855
time 929
corrupt index
  regenerating 1092
create a custom table
  create a table 355
  global default fields 360
create a UI policy
  convert a UI policy to a data policy 781
  view-specific UI policy 595
creating
  new field 716
crypto.policy parameter 2318
currency 793
  auditing 805
  conversion rate job 803
  conversions 802
  decimal places 805
  export 800, 821
  forms 797
  import 800, 821
  lists 798
  optimizer 806
  properties 803
  reference currency 795
  reports 798
  scripts 800
  session currency 795
custom tables
  delete 363
Customer feedback cloning 1535
customized objects
  during upgrades 2580
D
data archiving 1305
  affected records, verifying 1315
  archive rule, setting 1316
  archive schedule, changing 1321
  archived strings, language of 1315
  creating rules 1309
  related records 1312
  restored records, archiving 1325
  restoring 1321
  viewing 1316
data destruction
  creating rules 1315
Data Dictionary Tables 429
  system dictionary 432, 434
data import
  schedule 1469
  scripting options 1472
Data Lookup and Record Matching Support
  create a custom data lookup table 783
  create a data lookup module 788
  create custom data lookups 783
  data lookup definition record 785
  data lookup table 784
  data lookup value 784
  troubleshooting 789
data management 1301
data policy
  installed with 775
Data policy 775
  converting to a UI policy 781
  creating 776
  debugging 782
  fields 780
data preserver
  SAML properties 1524, 1723
data source 1367
  choice list 1381, 1382
  create 1383, 1670
Data Sources
  Custom CSV files 1374
  File 1367
  FTP extended properties 1377
  JDBC 1378
  LDAP 1386
database 1615
  Database Rotation 1538, 1540
database size 1615
Database Views
  add a table 469
  create a database view 468
  database views in the base system 479
  relabel a column 476
  specify a field to return 475
  specify number of records to return 476
  test the database view 477
  use disjunctions in complex queries 479
date and time fields 931
  configuring for the list editor 933
  personalizing the date format 932
  personalizing the time format 932
Date and Time Fields 930, 934, 935, 935, 935, 935, 936
daylight saving time
time zone 937
user preferences 937
default currency fields 793
default sort sequence
  list 488
define client scripts 599
delegation
  active directory application mode (ADAM) 1697
  ADAM 1697
delete
  custom tables 363
deleting all records
table 363
dictionary attributes 441
dictionary override
  define 433
dictionary overrides 433
Did You Mean?
suggestions, configuring 1057
digest token authentication
  enabling exit script 1800
  disabling
    attachment
table 557, 1101
drag-and-drop 555
  feature 555
table
  attachment 557, 1101
Discovery
  SCCM
    Asset Intelligence scheduled imports 1559
    SCCM integration
      switching versions 1559
disposition
  upgrade history 2577
Document ID Field 625
document scoring 1070
domain separation 979, 2447, 2449
  activating and deactivating domains 2546
  activating plugins 2530
  adding to a domain field 2546, 2551
  adding to a visibility domains list 2550
  applications 2466
  changing domain visibility 2550
  creating contains relationships between domains 2550
  creating domain-specific choice lists 2552
  default domain scope 2534
  delegated administration 2561
    example with domain specific applications and modules 2562
  domain assignment 2452
  domain scope 2456
  domain selection menus 2552
  domain visibility 2454
  enabling domain logging and debug messages 2568
  enabling the domain reference picker on UI15 2553
  enabling the domain reference picker on UI16 2552
  granting visibility domains to a group 2546
  granting visibility domains to a user 2551
  limitations 2466
  making a domain the default 2538
  manage MSP domains for records 2541
  properties 2534
  restricting access
    by role 2555
  selecting a primary domain 2536, 2547
  setup 2530
  user preferences 2534
  viewing historical messages 2569
  viewing MSP domain relationships 2546, 2556
  viewing real-time messages 2568
Domain separation 2552
domain separation for MSPs
  activating and deactivating domains 2546
  changing domain visibility 2550
  creating a domain 2536
installed components 2462
  making a domain the default 2538
  manage MSP domains for records 2541
  selecting a primary domain 2547
  viewing MSP domain relationships 2546, 2556
domain separation for schedule 979
domain separation setup 2569
domain support 979
drag-and-drop
  disabling 555
  feature 555
dynamic creation 680
E
e-signature approval
  SAML 2.0 authentication, setting up 1647
Easy Import
  add a record in the template 1496
  data type validation 1504
  import a record from the template 1498
  import template 1495
  paste data into the template 1502
  template type validation 1503
  template validation 1501
  update a record in the template 1497
Edge Encryption 2277, 2297, 2329, 2392, 2393, 2394
  adding proxies 2327
  attachment decryption job 2359
  attachment encryption 2358
  attachment encryption job 2358
  attachment key rotation job 2353
  attachments 2358
  configuration 2351
  configure 2397, 2397
  database recovery job 2362
  deactivate encryption 2355
  decryption job 2356
  dictionary attributes 2390
  digital signature 2315
  encryption application 2282
  encryption change 2360
  encryption deactivation 2355
  encryption job 2356
  encryption key management 2283
  encryption patterns 2360
  encryption proxy 2282
  encryption rule actions 2371
  encryption rule conditions 2370
  encryption rules 2367, 2370
  encryption type
    change 2360
    deactivate 2355
  encryption types 2286
  field encryption 2354
  file store 2322
  getting started 2289
  installation 2298
  installed components
    tables 2287
  installer 2301, 2302, 2305, 2306, 2306, 2310, 2311, 2312
  instance configuration 2354
History 1359
scheduled export scripting 1359
Export Sets
properties 1360
Exporting data
Exporting currency fields to Excel 1347
Exporting Data
export data 1330, 1332, 1335, 1336, 1338, 1338, 1348, 1350, 1351, 1352
extend 352
External Authentication (Single Sign-On - SSO) 1742, 1745, 1750, 1763, 1767, 1825

F
feature
  disabling 555
drag-and-drop 555
field
  add spell checking 664
creating
    new 716
field administration
  choice field search 620
  choice fields 620
Field administration
  normalize 743, 746, 748, 751, 753, 754, 755, 758
Field Administration
  choice lists
    change none display value 617
    customize 611
define option 615
delete 618
field type 619
remove none option 616
reuse 616
security 611
create a wikitext field 714
data lookup and record matching support 783, 783, 783, 784, 785, 788, 789
default choice lists
  integer values 612
extend functionality of a wikitext field 715
field normalization 735, 737
  supported wiki tags 713
use phone number fields 668, 668, 668, 668, 669, 669, 670, 671, 672, 673, 675, 677, 679, 679
values associated with choices
  scripting 612
wiki fields 713
Field map
  Script variables 1466
Field Normalization
  installed with 737
Field Normalization Rules
  expressions 772, 774
  patterns 772, 774
Field Styles
  defining 729
field transformations 758, 759
  create transformation records 760
  run data jobs 745, 745
  select transform types 761
test 762
field type
  create 740
fields
  HTML fields
    HTML sanitizer 2169, 2172, 2172, 2172, 2173, 2173
Fields
  creating new 716, 725, 727, 728
  introduction 725
file
  attachment 556
  role 556
file size
  attachment limiting 556
filter out
  hidden groups 1594
filters
  related list query blacklist 524
  restricting 501
  suppressing 501
Filters
  restricting 498
Financial Management
  fiscal calendar 958
  fiscal calendar generate 959
  view fiscal periods 961
fixed price fields 796
form administration
  create a UI policy 595, 595, 781
  create a UI policy example 598
  form design 528, 534, 534, 534, 536, 536
form annotations
  add 538
  language support 553
toggle 542
types 553
form design
  add a formatter 536
  add annotation 534
display field 534
new field 536
new section 534
form personalization
  activate 552
  administer 551, 552
disabling 552
manage 552
role requirements 552
user preferences 552
form section
  create 542
form splits
  add property to enable 601
form submission
double-check 2111
form templates 575
automatically applied 575
create from form 575
save form as template 581
scheduling 583
template bar 585
formatter 559
approval summarizer 570
create 561
create UI macro 559
override with macros 573
forms
activity formatter 561
live feed 563
add activity formatter 563
adding charts 549
adding related lists 538
annotate 553
configure 536
configure condition builder 622
configure customer updates indicator 549
configure insert for task records 599
control the label type 605
customize activities 564
define required fields 604
personalize 551, 552, 552, 552
personalizing 552
use HTML fields 642
frequency 1102

G
general security settings
properties 2069
Generate a certificate 1707
Glide
durations format
modifying 461
glide.history.role 2424
GlideElement 1797
global
print(String message) 2389
Global Catalog 1709
global text search 1050
search field 1043
search groups 1049
search preferences 1054
search result groups 1043
search suggestions 1057
Google
activating plugin 1547
grant role access
applications 1596
modules 1596
group type
add 1594
assign 1595
groups 1591
add a user 1593
create 1592
hide 1593
remove a user 1593

H
hidden field
group form 1593
hidden groups
filter out 1594
hierarchical list
enable 503
high security settings 2072, 2130
activating 2080
default deny property 2111
elevated privilege 2127
elevating to a privileged role 2131
forcing administrators to manually elevate 2132
history access
control 2417
history calendar 2419
history list 2418
history sets 2415
comparing CI snapshots 2426
differences with audit 2416
export historical CI snapshot 2426
HTML editor
paste options 656
HTML fields
embedding
images 652
video 654
image uploads 656
images
embedding 652
linking
website 654
TinyMCE deprecated tags 634, 635
TinyMCE HTML editor 633
TinyMCE HTML toolbar 633
video
defining file types 655
embedding 654
website
embedding 654
HTML Fields
TinyMCE version 4 editor 642
HTTP 500 error 346

I
icon
attachment
configuring 558
configuring
attachment 558
identity provider
Active Directory Federation Services 1755, 1755, 1757,
1757, 1757, 1762, 1762, 1763
IdP 1755, 1755, 1757, 1757, 1757, 1762, 1762, 1763
See also identity provider
image fields
using 656
images
embedding
HTML fields 652
Impersonate a User
force logout 1589
log impersonations 1588
on a mobile phone 1587
import data using import sets
Perl example 1474
post CSV or Excel files directly to an import set 1474
review the import set 1467
run import 1467
import log
viewing 1467
import run history 1468
Import Set Performance
troubleshooting 1505, 1505, 1506, 1506, 1506, 1507
import set tables 1564
web services 1565
import sets
performance improvements 1895
Import sets
Importing data using import sets 1438
maximum row size 1437
Import Sets 1361
Coalesce 1428
easy import 1494, 1495, 1496, 1497, 1498, 1501, 1502, 1503, 1504
properties 1477
web proxy 349, 350, 351, 351
Import sets properties 1477
importing
XML records 1508
Importing
ServiceNow instance 1507, 1509, 1509, 1510, 1510, 1511
XML records
matching existing records 1508
inactivity monitors
setting 999
index
field, removing 1093
HTML 1075
removing 1093
index suggestions for slow queries 1869, 1888, 1891, 1892
export to non-production instance 1878
generate 1873
review 1875
schedule index creation 1879
schedule index drop 1885
test index performance 1884
indexing 1088, 1099
install edge encryption 2314
installation exits 2137
Instance
translate 847, 848, 849, 849, 849, 850, 851, 853, 853, 854, 855, 856
instance locale
set 823
Instance Usage 1614
integrate 1541
Integrate
Edge Encryption 2391
integration 1541, 2392
Integrations 1542, 1566
available 1542
Internal CA, generate certificate 1707
Introduction to Fields 606
change 717
character counter 663
database field types 623
delete 718
delete multiple 718
field label 717
hint 717
IP address field type 657
text field 663
types 606
IP Range Based Authentication
access control 2152
J
Java digest algorithm
encryption 1803
JDBC driver
choice list, edit 1381, 1382
data source, create new 1383
DB2 1382
Install on a MID server 1383
Sybase 1382
JDBCPProbe 1568, 1568, 1568, 1570, 1571, 1573
job
schedule 996
journal fields 658, 660, 661, 661, 662, 662, 663, 663
configuring
suggested text 712
JSON API 2384
JsonNode 2384
encodedQueryFor(String tableName) 2388
getAsString() 2387
getAsString(String propertyName) 2387
getIterator(String xPath) 2386
getName() 2387
iterator() 2387
valueFor(String tableName, String fieldName) 2388
JsonNode API 2386
JsonNodeIterator
hasNext() 2389
next() 2389
JsonNodeIterator API 2389
K
keyword search 1102
L
language internationalization support 823
Choices table 832
configure a language as reading from right to left 827
Field Label table 830
global language 825
language table 827
Message table 829
service catalog buttons 856
Translated Name / Field table 828
Translated text 834
translation tables 826
user specific language 825
language plugin
activate 824
language support
form annotations 553
LDAP 1709
Active Directory 1678
assign field values 1678
binary data through mid server 1672
BLOB data 1672
common scripts 1678
connection monitoring 1671
create server 1657
deactivate 1678
exclude users 1679
extraction 1692
filters 1691
import maps 1673
inactive accounts 1692
integration 1649, 1652, 1654, 1655, 1656, 1670, 1671, 1674
error codes 1684
troubleshooting 1680
listener
setting up 1663
MID Server
troubleshooting 1672
notifications 1671
one-time password 1690
organizational unit 1667
OU 1667
refresh 1680
schema 1709
script 1678, 1678, 1679
script examples 1693
setup 1655, 1671
specifying attributes 1665
SSL certificate 1656
testing connections manually 1666
transform map 1674, 1680
user account
deactivate 1692
disabled 1692
user auto provisioning 1670
verify mapping 1680
X.509 certificate 1656
LDAP Connection Failed 1672
LDAP Monitor
view 1681
LDAP records
inactive 1690
synchronize 1690
LDAP transform
choice action 1679
create 1679
ignore 1679
reject 1679
LDAPs
ADAM 1699
certificate, assigning 1700
collection 1701
public key certificate 1700
self-signed certificate 1699
left-pad numbers
in custom tables 733
limiting
attachment
file size 556
file size
attachment 556
Linux 2327
list administration
list v3 519
disable for a table 527
disabling globally 526
enabling for related lists 526
list calculations 482, 525
list control 487
list control settings
for list editor 490
list controls 484, 487
list editor
 administering 489
contextual security, configuring 492
control settings, configuring 490
user preferences, managing 496
list editor properties
configure editable field types 490
disable list editing 490
list mechanic
access, controlling 497
activating 497
list v3
browser support 519
compatibility 520
debug compatibility 520
installed components
properties 521
lists
detail rows
enabling 498
locales 794
define 822
localization
form annotations 553
system 837
Localization
instance 847, 848, 849, 849, 849, 850, 851, 853, 853, 854, 855, 856
localization properties 837
location setup 837
Login
finding denied IP addresses 2153
IP range based authentication 2151, 2152, 2153
login landing page
specifying 2135
Login Scenarios 2134
login security 2133
activating ServiceNow access control 2086
configuring ServiceNow access control 2088
ServiceNow access control 2083
logout button
remove 2137
logout confirmation prompt
enable 2136

M
Managing Data
system clone 1512, 1515, 1518, 1519, 1522, 1534, 1536
manually install
proxy server 2314
Many to Many Task Relations
define a relationship type 425
define a task relationship allowed 426
mark as solution button 427
modify the displayed field 427
plugin manifest 424
request the plugin 422
task relationship type record 426
ui actions 427
many-to-many relationship
creating 466
referencing 467
match relevance by
field, controlling 1072
Metric Definition Support
metric definition 1851
metric instance 1853
sample field value duration script 1852
metric definitions 1005
Microsoft
SMS/SCCM integration 2.0 1549
Microsoft Active Directory, configure SSL access 1706
Microsoft SCCM
configuration 1555
schedule 1555
MID Server 1671
configure 2397, 2397
integrate Edge Encryption 2397, 2397
modify form focus 600
multi-tenancy 2447, 2449, 2466
multiple fields
sort 489
multiple price fields 796
Multiple Provider
single sign-on 1648
using with ESS 1646
Multiple provider SSO 2329
MySQL global status 1913

N
navigation and UI
context menu 513, 518, 518, 519
new customizations
translate 840
new department
adding 1581
Non-Interactive Sessions 1612, 1613, 1614, 1614, 1614
Nonce
implementing 2153, 2153, 2154
normalization
company name 1850
properties 1850
Normalization Data Services 1850
number of history entries
change 2417

O
OAuth
activating 1782
APIs 1798
scoped 1798
authorization code flow 1790
authorization code grant flow 1790
authorize access 1793
external client scenario 1782
manage OAuth tokens 1795
profile
parameters 1786, 1787
property 1782
revoking a token 1796
setting up 1781
OAuth 2.0 1780
authorization code flow
instance as authorization server 1794
ODBC Driver 2392, 2394
ODBC truststore 2393
on load check box 599
OpenLDAP
modify 1710
order-preserving database 2311
Order-preserving encryption 2294
organizational unit
ADAM 1697
create 1697

P
pages
make public 2136
parallel processing
configuring 1052
ParameterValue
encodedQueryFor(String tableName) 2377
toString() 2375
valueFor(String tableName, String fieldName) 2377
parent record 576
password reset 2141
notification 2143
Password Reset
properties 2143
user lockout 2135
password validation rules
strengthen 2140
pause conditions 999
Percent Complete Field 666, 666, 667
performance
evaluating 1864
performance metrics 1896
AMB graphs 1905
database graphs 1906
MySQL global status graphs 1913
replication throughput 1906
slow pattern graphs 1918

personal lists
  administering 497
  managing 497
personalizing lists 481, 481, 482, 484, 487, 488
  list calculations 482, 525

Personalizing Lists 487
Planned Task 383, 383, 384, 386, 387, 388, 390
Planned Task Hierarchy 389
Platform encryption 2262
Platform Performance
  Stats Tools plugin 1864
  table extension 1938
  troubleshoot performance 1855, 1856, 1858, 1860
Platform security
  overview 1940
Plugin
  Google custom search integration 1547
plugins
  activate 14
  general 14
  options for activating 14
Plugs
  List of Plugins 19
pop-up information
  customize 690
Portal
  Time Sheet 398
  preserve applications 1527
  price fields 796
  process flow formatter 567
  activating 568
  create 568
Production System 1561
  properties 1050, 2394
  properties module
    creating 345
proxy database 2311
Proxy database
  size 2294
Proxy Error Reports 2397
Proxy performance dashboard 2397
proxy server 2392
  set initial memory 2325
  set memory 2325
  set upper bound memory 2325
proxy server installation 2314
public key certificate
  exporting 1700
  LDAPS 1700
Public key certificate, export 1708
punctuation 1073
purchase plugins 14
put the class name here 1797

Q

query method
  configuring 1052
query mode
  single table 1094
quotas
  application 1935
  application properties 1936
  transaction 1927

R

range calculator scripts 1018
ranking
  stories 512
read only role 1603
read-only fields
  pop-ups 690
record
  deleted 1710
Record Numbering
  managing 731, 731, 733, 734
records lists
  enable text searches 1075
  text searches 1058
recovery
  active directory application mode (ADAM) 1699
  ADAM 1699
Recurring cloning 1531
redundancy
  active directory application mode (ADAM) 1699
  ADAM 1699
reference autocompletes
  using wildcards 708
reference currency 795
Reference Field
  auto-complete 700
reference fields 679
  add 680
  dynamic creation 680
  recent selections 709
Reference Fields
  auto-complete 683, 702, 703, 704, 705, 707
  cascade delete rules 681
  decorations 685
  define reference key 682
  display values 684, 684
  lookup 685, 687
  reference icon 688
  related incidents icon 691
  select 684
  show workflow icon 691
  tree picker 687
reference qualifiers 692, 697, 698, 699, 700
registering
  event 998, 1300
related list
  select 505
related list query
  blacklist system property 524
related lists
  enabling list v3 526
related record 576
related tables 352
relative duration
  define 1026
  use 1027
Remember Me check box 2151
  default value, changing 2151
  removing 2151
reminder 391
Repeat cloning 1515, 1531
request
  getAsJsonContent() 2372, 2376
  getAsXmlContent() 2373, 2376
  XMLContains(String path) 2373
request API 2372
request plugins 14
resolve conflicts 2580, 2588
restore deleted records
  configure 2414
  deletion audit 2414
  system table 2414
restoring deleted records and references 368
restrict a field
  example 494
  with a condition, example 496
  with a script, example 495
restrict a table
  example 493
role
  attachment
    file 556
  file  attachment 556
role delegation 1605, 1605
prevention 1606
roles 1595
  acl rules 1606
  create 1595
  group
    assign role 1597
    creating 1596
    security jump start 1606
Roles
  base system roles 1598, 1602
  RSA key pair 2305
S
SAML 1629
  2.0
    Java keystore 1737
    profile 1636, 1641, 1722, 1725, 1726, 1727, 1727, 1727, 1728, 1728, 1729, 1729, 1730, 1730, 1730, 1731, 1731, 1732, 1736, 1738, 1739, 1739, 1745, 1747, 1751, 1753, 1754, 1754, 1754, 1764, 1765, 1768
    SSO 1636, 1641, 1722, 1725, 1726, 1727, 1727, 1727, 1728, 1728, 1729, 1729, 1730, 1730, 1730, 1731, 1731, 1732, 1736, 1738, 1739, 1739, 1745, 1747, 1751, 1753, 1754, 1754, 1764, 1765, 1768
    SAML 1.1
    migrating 1764
    SAML 2.0
      integration with other features 1754
      troubleshooting 1766
Sample C 1804
SCCM
  Asset Intelligence scheduled imports 1559
  switching versions 1559
schedule
  calendar 977
Schedule cloning 1515
schedule domain separation 979
schedule domain support 979
schedule script execution 990
scheduled data import
  time zone 940
scheduled job 982
Scheduled jobs 981
scheduled report 983
scheduled reports
  time zone 940
Schedules
  using 961, 962, 965, 965, 965, 965, 969, 969, 971, 973
Scoped GlideElement 1797
script actions 1295
script includes
  suppress breadcrumbs and filters 501
script sandboxing 2079
search 1028, 1042
  attachments 1099
  phrase searches 1062
  wildcards 1063
search groups 1046
search phase 1063
search phases 1063
search process 1063
search provider
  build 1575
  search results 1046
searching
  boolean operators 1060
Searching
  Google 1547
security
  active directory application mode (ADAM) 1694
  activity formatter 561
security admin 2130
security_admin 2130
self-service password reset 2141
self-signed certificate 2393
ADAM 1699
LDAPS 1699
Server Scripting
  transform map scripts 1410, 1412, 1414
Service Catalog
  localizing price 803, 836
  service level agreements
    timing 1005
ServiceNow
  intranet 1568
ServiceNow Access Control
  audit logging 2089
ServiceNow servlet 1915
ServiceNow Store Usage Overview 1615
  session currency 795
  set up VPN
    ServiceNow and business network 2445
signature key
  configure 2305
single logout
  Active Directory Federation Services 1762
  single sign-on
    multi-provider 1618, 1623, 1635
      activating 1620
      choosing the IdP 1645
      configuring users 1629, 1637
      IdPs 1637
      installed with 1619
      logging in 1644
      modifying the primary 1629, 1637
      setting up 1621
      testing connections 1637
      troubleshooting scripts 1644
      troubleshooting test connections 1641
Single sign-on
  digest token authentication 1799
    creating links 1802
    entering multi-provider single sign-on properties 1801
    entering single sign-on properties 1800
    generating a digest token 1800
    sample implementation 1803
    testing the integration 1799, 1799, 1802
  single-currency mode 795
size limits
  joins 349
skipped updates 2580
slow query logs
  use 1867
Solutions 1203
sort order
  remember 489
spans 1021
spell checking
  add to a field 664
SSL access, configure Microsoft Active Directory 1706
stand-alone CA, set up 1707
Standard Import Set Tables 1430
statistics
  text indexing 1095
Stats Tools
  performance evaluation 1864
status
  text indexing 1095
stop words
  automatic, configuring 1104
  global, configuring 1103
  table-specific, configuring 1103
stories
  ranking 512
string fields
  configuring
    suggested text 711
  suggestion fields
    adding 710
Support
  encryption 2257, 2262, 2264, 2266, 2267
  synchronize
    LDAP records 1690
  synonym dictionaries 1106
  synonym dictionary 1107
  synonym search
    debug 1107
sys audit table
  understanding 2412
syslog probe 1576
system clone 1527
SAML integration 1524, 1723
System clone
  exclude a table from cloning 1519
  start a clone 1515
System Clone
  create a clone target 1518
  preserve data 1522
  run post clone cleanup scripts 1536
  view active clones 1534
  view clone history 1534
system diagnostics
  running 1860
system dictionary
  modifying 434
System Dictionary
  dictionary entries 434
  system localization 837
  system log messages 1934
system logs
  restore deleted records 2414
  system properties 261
    adding 344
  System Scheduler 981
T
  tabbed forms
    display 545
  table 391, 1088
    attachment
      disabling 557, 1101
      viewing 553
deleting 362
disabling
  attachment 557, 1101
table administration 352
    restoring deleted records and references 368
    unique record identifier 1304, 1304, 1305
Table Extension example 1938
  table field
    prevent auditing 2414
  table hierarchy
    extension model 1925
  table index 370
  table rotation 1920
  table rotations
    apply 1920
  tables
    delete 363
Tables
  schema map 463, 463, 464
  tables module 360
  task parent breadcrumbs formatter 569, 570
  customize 570
  task table 391
  flattening 1924
Task table 576
  activate time cards 393
  copy time cards 415
  creating a task 370
  important Task table fields 378
  journal fields 381
  modifications 392
  Planned Task plugin 370
  time cards 392, 412, 413, 418, 419
  time sheet policies 393
  time sheets 409
  tools for driving tasks 420
Task Table
  assignment lookup rules example 372
  assignment module rule 374
  assignment rules 373
  assignment rules module 372
  baseline assignment rules example 374
  business rules 373
  condition editor example 372
  data lookup rules 373, 377
  defining assignment rules 371
  many to many task relations 422, 422, 424, 425, 426, 427, 427, 427
  workflow assignments 373
tasks
  tasks workflow 392
template 576
  apply from a module 583
  scripting 586
Test LDAPS connectivity 1708
  text index 1088
text indexing
    statistics 1095
    status 1095
TF-IDF scoring 1071
  third-party 1541
threads
  performance monitoring 1895
time
  display 1000
  scheduled jobs 997
Time
  time zones 939
  view system logs 1292, 2410, 2429, 2430, 2433, 2435, 2436, 2436, 2436, 2437, 2437
Time card
  submit time card 417
  time card management 392
    time cards 392
    time sheet policies 393
Time card management
  approve time sheet 411
  assign time sheet policy to a user 397
  create time sheet 410
  create time sheet policy 393, 409
  reject time sheet 411
  set time sheet policy as default policy 397
  submit time sheet 411
  time cards 412
  Time Sheet Portal 398
  time sheets 409
time cards
  approve time card 418
  reject time card 418
  time sheet policies 393
  time sheets 409
Time Cards
  create time cards 416
  create time sheet policy 393
  tools for driving tasks 420
time sheet portal
  approve time sheet for your resources 409
  submit a time sheet for your resources 409
Time Sheet Portal
  Create time cards 407
  log time 407
  submit time sheet 408
time sheets
  approve time card 418
  approve time sheet 411
  approve time sheet for your resources 409
  create time sheet policy 393
  reject time card 418
  reject time sheet 411
  set time sheet policy as default policy 397
  submit a time sheet for your resources 409
  submit time card 417
  submit time sheet 411
time cards 412
Time Sheets
  copy time cards 415
  create time cards 413
time worked fields 1005
time zone
  choice list 939
  scheduled data import 940
  scheduled reports 940
time zones
daylight saving time 937

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
email notification 937
scripting 937
service level agreement 937
user preferences 937
Timeline Pages 1003, 1006, 1011, 1011, 1013, 1014
timelines 1021, 2424
Timelines
using 1020, 1020
timing functionality 1005
TinyMCE HTML deprecated tags 634, 635
TinyMCE HTML editor 633
TinyMCE HTML toolbar 633
Tokenization 2294
transaction
cancel timer 1893
canceling 1893
transaction quotas 1927
transactions
canceled 1894
logging 1894
transform category
create 772
transform definitions 764, 767, 768
create 767
transform map
create 1457
Transform Map Scripts
event scripts 1414
transformation script variables 1410
Transform Maps
creating 1408, 1458, 1463
translate and learn property
use 845
Translated Text 851, 853
translation prefix
display 835
Troubleshoot Performance
compression 1860
network response times 1858
response time on forms 1856
transaction log response times 1855
Type
Rate 398
type ahead
suggestions, updating 1057
U
ui actions 488
UI actions 587, 590, 592, 593, 594
UI policies
client scripts 599
UI policy
creating from a data policy 781
unique record identifier 1304
untranslated string
export 841
upgrade
proxy server 2348
Upgrade History 2577, 2588
upgrade monitor
upgrade platform 2590
upgrade system 2590
Upgrade Monitor />
upgrade instance 2590
upgrades 2577
Use HTML Fields
editing functions 640
extended functions 638
formatting 636
highlight text in the TinyMCE editor 649
insert a line break 649
style a table 650
Use Phone Number Fields
configure e.164 phone number fields 668
dependent fields 668
display of local format 669
e.164 phone number field dictionary attributes 675
e.164 phone number field system properties 673
entry of international format 669
international direct dialing prefix 672
phone formats 679
phone territory selector choice list 670
phone validations 679
territories assigned 668
territory format validation 668
territory labels 671
territory phone display rule 677
Use Time Zones
set a system time zone 939
User administration
company 1580
user preferences 1584
list editor, managing 496
user registration 1586
approve an account 1586
enable auto processing 1579
user sessions
locking out a user 1591
making a user inactive 1591
managing 1589
terminating a user session 1591
User sessions
modify session timeout 1590
users
allow to view a profile 1579
assign roles 1597
create 1581
Users and Groups
impersonate a user 1587, 1588, 1588, 1588, 1589
Using Forms
use HTML fields 632, 636, 638, 640, 649, 649, 650
V
validation script
deactivate 1583
Verizon
ebonding
migrating 1561
integration 1561
video
defining file types
  HTML fields 655
embedding
  HTML fields 654
view cmdb ci 2424
View System Logs
  audited tables 2410
  customer updates table 2436
  email logs 2433
  event logs 1292, 2435
  import logs 2436
  log history 2437
  log utilities 2437
  system diagnostics application 2436
  system logs 2429
  transaction logs 2430
viewing
  attachment
    table 553
  table
    attachment 553
VPN communication
  create address 2447
VPN service
  request 2447

W
watch lists
  configure email notifications 719
  configure order buttons 719
  hide email addresses 719
  use 718
Web Proxy
  ntlm authentication 350
  proxy servers 351, 351
  soap clients 351
Web service import sets 1484, 1488, 1490
Web Service Import Sets 1483
  Security requirements 1491
web service security 2162, 2163, 2166
website
  HTML fields
    linking 654
    linking
      HTML fields 654
words 1073

X
XML API 2377
XML files
  export 1353
  import 1353
XML Files
  exporting 1330
  importing 1330
XML import sets 1509
XmlContent 2377

© 2021 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.