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 ........................................................................... 7
  Activate a plugin ............................................................................. 7
  Find components installed with an application ................................ 116
  Using guided setup ........................................................................ 117
  Available system properties ............................................................ 123
  Handle HTTP 500 errors ................................................................ 204
  Query join and complexity size limits ............................................. 206
  Tables and classes .......................................................................... 207
  Web proxy ..................................................................................... 213
Table administration .......................................................................... 216
  Table extension and classes ............................................................ 216
  Create a table ................................................................................ 219
  Tables module ............................................................................... 225
  Delete a table ................................................................................ 227
  Delete all records from a table ....................................................... 227
  Roll back and delete recovery ......................................................... 230
  Create a table index ..................................................................... 234
  Task table ..................................................................................... 234
  Data dictionary tables .................................................................... 289
  Schema map for tables ................................................................. 322
  Create a many-to-many relationship .............................................. 325
  Database views ............................................................................. 326
List administration ............................................................................ 336
  List configuration .......................................................................... 336
  Controlling the sort sequence used to display lists ......................... 343
  List editor administration .............................................................. 344
  Personal list administration .......................................................... 352
  Administer detail rows .................................................................. 353
  Restrict filters and breadcrumbs with fixed queries ....................... 353
  Enable a hierarchical list ................................................................ 358
  Context ranking ............................................................................ 361
  Customize List v2 context menus .................................................. 368
  List v3 administration ................................................................... 373
Form configuration ............................................................................. 382
  Using the form designer ............................................................... 382
  Configuring the form layout .......................................................... 390
Form administration .......................................................................... 402
  Administering form personalization .............................................. 403
  Administering form annotations .................................................. 405
  Administering attachments .......................................................... 406
  Formatters ................................................................................... 411
  Form templates ............................................................................ 427
  UI actions .................................................................................... 439
  UI policies ................................................................................... 448
  Advanced form configuration ....................................................... 452
Field administration .......................................................................... 459
  Field types ................................................................................... 459
  Add and customize a field in a table ............................................ 557
  Field normalization and transformation ....................................... 573
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data policy</td>
<td>610</td>
</tr>
<tr>
<td>Data lookup and record matching support</td>
<td>618</td>
</tr>
<tr>
<td>State Management</td>
<td>624</td>
</tr>
<tr>
<td>Add a state model and transitions</td>
<td>625</td>
</tr>
<tr>
<td>Implement process flow and UI actions with a state model</td>
<td>627</td>
</tr>
<tr>
<td>Installed with State Model</td>
<td>627</td>
</tr>
<tr>
<td>Currency administration</td>
<td>629</td>
</tr>
<tr>
<td>Locale settings</td>
<td>629</td>
</tr>
<tr>
<td>Session and reference currency</td>
<td>629</td>
</tr>
<tr>
<td>Single-currency mode</td>
<td>631</td>
</tr>
<tr>
<td>Price fields</td>
<td>631</td>
</tr>
<tr>
<td>Currency values in lists</td>
<td>632</td>
</tr>
<tr>
<td>Currency values in forms</td>
<td>633</td>
</tr>
<tr>
<td>Currency values in reports</td>
<td>634</td>
</tr>
<tr>
<td>Currency conversions</td>
<td>634</td>
</tr>
<tr>
<td>Currency values in import and export</td>
<td>635</td>
</tr>
<tr>
<td>Currency values in scripts</td>
<td>636</td>
</tr>
<tr>
<td>Configure currency fields in audit records</td>
<td>638</td>
</tr>
<tr>
<td>Change currency decimal places</td>
<td>639</td>
</tr>
<tr>
<td>Configure currency optimizer</td>
<td>639</td>
</tr>
<tr>
<td>Currency system properties</td>
<td>639</td>
</tr>
<tr>
<td>Localization settings</td>
<td>641</td>
</tr>
<tr>
<td>Define locales</td>
<td>641</td>
</tr>
<tr>
<td>Internationalization support</td>
<td>642</td>
</tr>
<tr>
<td>Localize price fields</td>
<td>655</td>
</tr>
<tr>
<td>Use translated text</td>
<td>655</td>
</tr>
<tr>
<td>System localization</td>
<td>657</td>
</tr>
<tr>
<td>Time configuration</td>
<td>665</td>
</tr>
<tr>
<td>Date and time fields</td>
<td>665</td>
</tr>
<tr>
<td>Calendars and schedules</td>
<td>671</td>
</tr>
<tr>
<td>Client transaction timings</td>
<td>694</td>
</tr>
<tr>
<td>Define a relative duration</td>
<td>697</td>
</tr>
<tr>
<td>Time display</td>
<td>699</td>
</tr>
<tr>
<td>Time-related functionality</td>
<td>702</td>
</tr>
<tr>
<td>Range calculator scripts</td>
<td>703</td>
</tr>
<tr>
<td>Set an inactivity monitor</td>
<td>706</td>
</tr>
<tr>
<td>System scheduler</td>
<td>707</td>
</tr>
<tr>
<td>Event scheduling</td>
<td>714</td>
</tr>
<tr>
<td>Timeline pages</td>
<td>715</td>
</tr>
<tr>
<td>Timing functionality</td>
<td>729</td>
</tr>
<tr>
<td>Time zones</td>
<td>730</td>
</tr>
<tr>
<td>Search administration</td>
<td>734</td>
</tr>
<tr>
<td>Features of search administration</td>
<td>735</td>
</tr>
<tr>
<td>Zing text indexing and search engine</td>
<td>735</td>
</tr>
<tr>
<td>Contextual search displays matching knowledge results</td>
<td>786</td>
</tr>
<tr>
<td>Events</td>
<td>823</td>
</tr>
<tr>
<td>Event registry</td>
<td>824</td>
</tr>
<tr>
<td>Event states</td>
<td>824</td>
</tr>
<tr>
<td>Event logs</td>
<td>825</td>
</tr>
<tr>
<td>The incident events business rule</td>
<td>825</td>
</tr>
<tr>
<td>Sample scripts from the change events business rule</td>
<td>827</td>
</tr>
<tr>
<td>Script actions</td>
<td>828</td>
</tr>
<tr>
<td>Global events</td>
<td>831</td>
</tr>
<tr>
<td>Create an event</td>
<td>832</td>
</tr>
<tr>
<td>Register an event</td>
<td>833</td>
</tr>
<tr>
<td>Reprocess an event</td>
<td>834</td>
</tr>
</tbody>
</table>
Pass event parameters from a workflow to a notification .................................................. 834
Data management .................................................................................................................. 835
The unique record identifier (sys_id) .................................................................................. 837
Data archiving ...................................................................................................................... 838
Export and import XML files .............................................................................................. 853
Export sets ............................................................................................................................ 877
Import sets ............................................................................................................................ 883
System clone .......................................................................................................................... 990
Database rotation .................................................................................................................. 1007
Domain separation and Data Management ......................................................................... 1010
Integration with third-party applications and data sources ................................................. 1010
Integration options .............................................................................................................. 1011
User administration ............................................................................................................. 1045
Manage user administration system properties ................................................................. 1045
Add a new company ............................................................................................................. 1046
Add a department ............................................................................................................... 1047
Create a user ......................................................................................................................... 1048
User self-registration .......................................................................................................... 1052
Impersonate a user .............................................................................................................. 1053
Manage user sessions ........................................................................................................ 1056
Groups .................................................................................................................................. 1058
Skills Management ............................................................................................................. 1061
Roles ..................................................................................................................................... 1063
Non-interactive sessions ..................................................................................................... 1082
Instance Usage ..................................................................................................................... 1084
Authentication ...................................................................................................................... 1087
Normalization Data Services ............................................................................................... 1260
Metrics .................................................................................................................................... 1263
Create a metric .................................................................................................................... 1264
Sample field value duration script ..................................................................................... 1265
Metric instance .................................................................................................................... 1266
Platform performance ......................................................................................................... 1268
Transaction log response times ......................................................................................... 1268
Network response times ..................................................................................................... 1271
Browser settings and performance ..................................................................................... 1273
Diagnostics page .................................................................................................................. 1273
System Diagnostics Stats Tools ......................................................................................... 1277
Use a slow query log ............................................................................................................ 1280
Index suggestions for slow queries ................................................................................... 1281
Transaction cancellation ...................................................................................................... 1297
Import set performance ........................................................................................................ 1299
Thread performance monitoring ....................................................................................... 1300
Performance metrics ........................................................................................................... 1301
Table rotation ....................................................................................................................... 1321
Table flattening ................................................................................................................... 1328
Add a module to test connection speed ............................................................................. 1330
This ServiceNow instance ................................................................................................. 1331
Transaction quotas ............................................................................................................. 1333
Application quotas .............................................................................................................. 1341
Use table extension ............................................................................................................. 1344
Upgrades and conversions ................................................................................................. 1345
Upgrade History module: Track every upgrade ................................................................. 1346
Upgrade Monitor module: Upgrade an individual instance ............................................... 1357
Debug upgrade .................................................................................................................... 1375
Express conversion to ServiceNow Enterprise ................................................................. 1378
Platform security ............................................................................................................... 1384
Now Platform Administration

The primary administrator role (admin) has access to all system features, functions, and data, regardless of security constraints. Additional administrator roles manage specific applications.

ServiceNow administrators can configure the system in many different ways to address the business needs of an organization. They can install and set up any number of the process applications that are provided with ServiceNow and also create custom applications. Applications can be made available to selected users by way of roles and other access controls. The system may also be configured to send and receive notifications as a way to create and track service requests.

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.

Activate a plugin

You can activate most plugins. Some features require a separate subscription from the rest of the Now Platform. Some plugins require a purchased subscription before activation. Some plugins must be activated by ServiceNow personnel.

Role required: admin

For evaluation, you can activate the plugin for an application that requires a purchased subscription on a non-production instance. To activate the plugin on production instances, you must purchase the subscription. To purchase a subscription, contact your ServiceNow account manager. For details on purchasing a plugin, see Purchase a plugin.

Some plugins require activation by ServiceNow personnel. Request these plugins through the HI Customer Service System instead of activating them yourself. For details, see Request a plugin.

For plugins that you can activate yourself, continue with the following steps.

1. Navigate to **System Definition > Plugins**.
2. Find and click the plugin name.
3. On the System Plugin form, review the plugin details and then click the **Activate/Upgrade** related link.

   - If the plugin depends on other plugins, these plugins are listed along with their activation status.
   - If the plugin has optional features that depend on other plugins, those plugins are listed under some files will not be loaded because these plugins are inactive. The optional features are not installed until the listed plugins are installed (before or after the installation of the current plugin).
4. Optional: If available, 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 practice when you first activate the plugin on a development or test instance.

You can also load demo data after the plugin is activated by clicking the **Load Demo Data Only** related link on the System Plugin form.

5. Click **Activate**.

### List of plugins (London)

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 HI 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 London release](#).

<table>
<thead>
<tr>
<th>Plugin ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.glide.ui_activity_formatter</td>
<td>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>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>Inactive</td>
<td>false</td>
<td>com.snc.app.agent_calendar</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
</tr>
<tr>
<td>--------</td>
<td>----</td>
<td>-------------</td>
<td>-------</td>
<td>---------------</td>
</tr>
<tr>
<td>Agile Development 2.0</td>
<td>com.snc.sdlc.agile.development</td>
<td>Agile Development 2.0 plugin provides enhanced functionality on top of Agile Development. If you already have a customized version of Agile Development, delete the customizations before activating “Agile Development 2.0” to ensure that all features work properly. Please refer the documentation for detailed steps to delete the customizations.</td>
<td>Inactive</td>
<td>true</td>
</tr>
<tr>
<td>Anonymous Connect Support</td>
<td>com.glide.connect.support</td>
<td>Plugin to enable access and properties for Anonymous Connect Support.</td>
<td>Inactive</td>
<td>false</td>
</tr>
<tr>
<td>API Analytics</td>
<td>com.glide.api_analytics</td>
<td>Admins to view API Analytics statistics for web services.</td>
<td>Active</td>
<td>false</td>
</tr>
<tr>
<td>API Stats</td>
<td>com.glide.stats</td>
<td>API Stats</td>
<td>Active</td>
<td>false</td>
</tr>
<tr>
<td>App APIs (New in London)</td>
<td>com.glide.app_api</td>
<td>APIs for fetching Application and Application Rollback related information.</td>
<td>Active</td>
<td>true</td>
</tr>
<tr>
<td>App Dependency</td>
<td>com.sn.dependency</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>
</tr>
<tr>
<td>Plugin Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
<td></td>
</tr>
<tr>
<td>--------------------</td>
<td>---------</td>
<td>----------------</td>
<td>--------------</td>
<td></td>
</tr>
<tr>
<td>Application Authorization</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.ui.angular, com.glide.ui.heisenberg</td>
<td></td>
</tr>
<tr>
<td>Application Creator</td>
<td>Retired</td>
<td>false</td>
<td>com.glide.ui.angular, com.glide.ui.heisenberg</td>
<td></td>
</tr>
<tr>
<td>Application Creator Templates</td>
<td>Active</td>
<td>false</td>
<td>com.glide.ui.angular, com.glide.ui.heisenberg</td>
<td></td>
</tr>
<tr>
<td>Application Design Restrictions</td>
<td>Active</td>
<td>false</td>
<td>com.glide.ui.angular, com.glide.ui.heisenberg</td>
<td></td>
</tr>
<tr>
<td>Application File</td>
<td>Active</td>
<td>false</td>
<td>com.glide.ui.angular, com.glide.ui.heisenberg</td>
<td></td>
</tr>
<tr>
<td>Application Metadata</td>
<td>Active</td>
<td>false</td>
<td>com.glide.ui.angular, com.glide.ui.heisenberg</td>
<td></td>
</tr>
<tr>
<td>Application Portfolio Management</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.sp_workbench_widgets, com.snc.financial_planning, com.snc.fiscal_calendar, com.snc.treemap</td>
<td></td>
</tr>
<tr>
<td>Application Service (New in London)</td>
<td>Active</td>
<td>false</td>
<td>com.snc.itom.ui, com.snc.cmdb, com.snc.cmdb.service.modeling, com.glide.ui.list_v3_components</td>
<td></td>
</tr>
<tr>
<td>Plugin 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>
</tr>
<tr>
<td>App. Access Control</td>
<td>Implements file-level access for application development.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.apps, com.snc.apps_picker</td>
</tr>
<tr>
<td>App. 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>Applies changes, 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 (New in London)</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 (New in London)</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>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>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, com.glideapp.workflow, com.glideapp.survey, com.snc.bestpractice.task_survey, com.glide.survey_designer</td>
</tr>
<tr>
<td>Assessment Designer</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.snc.assessment_designer.common, com.glide.assessment_designer.common, com.glide.assessment_designer.module</td>
</tr>
<tr>
<td>Assessment Designer</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.module</td>
</tr>
<tr>
<td>Plugin 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>
</tr>
<tr>
<td>Assessment Designer Common</td>
<td>com.glide.assessment_designer.common</td>
<td>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>
</tr>
<tr>
<td>Asset Management</td>
<td>com.snc.asset_management</td>
<td>Manage all your assets, consumables, and software licenses.</td>
<td>Active</td>
<td>true</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>
</tr>
<tr>
<td>Auto Recovery</td>
<td>com.glide.autorecovery</td>
<td>Enable Auto Recovery functionality.</td>
<td>Active</td>
<td>false</td>
</tr>
<tr>
<td>Automated Test Framework - Application Navigator (New in London)</td>
<td>com.glide.automated_testing_impl.left_nav</td>
<td>Provides Testing steps that validate access to the application navigator.</td>
<td>Active</td>
<td>false</td>
</tr>
<tr>
<td>Automated Test Framework - REST Inbound</td>
<td>com.glide.automated_testing_impl.rest_inbound</td>
<td>Automated Test Framework for inbound REST requests.</td>
<td>Active</td>
<td>true</td>
</tr>
<tr>
<td>Plugin ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependence</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
<td>------------</td>
</tr>
<tr>
<td>automated_test_framework_schedule</td>
<td>Automated Test Framework - Schedule</td>
<td>Active</td>
<td>false</td>
<td>com.glide.automated_testing_impl.schedule</td>
</tr>
<tr>
<td>automated_test_framework_wce</td>
<td>Automated Test Framework - Whitelisted Client Errors (New in London)</td>
<td>Active</td>
<td>false</td>
<td>com.glide.automated_testing_framework</td>
</tr>
<tr>
<td>automated_test_framework_service_catalog</td>
<td>Automated Test Framework Service Catalog</td>
<td>Active</td>
<td>true</td>
<td>com.glide.automated_testing_framework, com.glideapp.servicecatalog</td>
</tr>
<tr>
<td>automated_test_framework_service_catalog_portal</td>
<td>Automated Test Framework Service Catalog Service Portal (New in London)</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>Automated Test Framework Service Portal (New in London)</td>
<td>Active</td>
<td>false</td>
<td>com.glide.automated_testing_framework</td>
</tr>
<tr>
<td>automatic_assignment</td>
<td>Automatic Assignment</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>basic_export_set_functionality</td>
<td>Basic Export Set Functionality</td>
<td>Active</td>
<td>false</td>
<td>com.glide.system_export_set</td>
</tr>
<tr>
<td>benchmark_client</td>
<td>Benchmark Client</td>
<td>Active</td>
<td>false</td>
<td>com.sn_bm_common</td>
</tr>
<tr>
<td>Plugin Description</td>
<td>ID</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------------------</td>
<td>----</td>
<td>-------</td>
<td>---------------</td>
<td>--------------</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>
</tr>
<tr>
<td>Benchmark Spoke</td>
<td>com.sn_bm_spoke</td>
<td>Spoke the evaluation framework for Benchmarks Recommendations.</td>
<td>Active</td>
<td>false</td>
</tr>
<tr>
<td>Best Practice - Bulk CI Changes</td>
<td>com.snc.bestpractice.bulkchange</td>
<td>Simple CI change 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>
</tr>
<tr>
<td>Best Practice - Change Risk Calculator</td>
<td>com.snc.bestpractice.changerisk</td>
<td>Simple risk and impact calculations for change management.</td>
<td>Active</td>
<td>false</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>
</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>
</tr>
<tr>
<td>Business Rule V2</td>
<td>com.glide.business_rule_v2</td>
<td>Business rules to support script-free conditions and behaviors.</td>
<td>Active</td>
<td>false</td>
</tr>
<tr>
<td>Cache build stats</td>
<td>com.glide.stats_cache_build_stats</td>
<td>Cache build stats.</td>
<td>Active</td>
<td>false</td>
</tr>
<tr>
<td>Plugin 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>
</tr>
<tr>
<td>Case Assignment Workbench Demo</td>
<td>Designed 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.demo, com.snc.assignment_workbench</td>
</tr>
<tr>
<td>Catalog Designer Common</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>Active</td>
<td>false</td>
<td>com.glide.ui.ng.dc, com.glideapp.workflow</td>
</tr>
<tr>
<td>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>Centralized Connection and Credential components.</td>
<td>false</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Certification 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                     | Active   | false          | com.glide.list_v2, com.snc.version                                           |
<p>| Change Management - CAB Workbench | Change Management feature which allows CAB Managers to schedule, plan and manage CAB Meetings all on the NOW platform. | Active   | true           | com.snc.change_management, com.snc.app.calendar, com.glide.service-portal, com.snc.app_common.service_portal, com.glide.editor.tinymce |</p>
<table>
<thead>
<tr>
<th>Plugin ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Management - Collision Detector</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 (New in London)</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>
</tr>
<tr>
<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_request_active, com.snc.change_request_inactive, com.snc.change_request_collision |
<table>
<thead>
<tr>
<th>Plugin ID</th>
<th>Plugin Name</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.snc.change_management.standard_change_catalog</td>
<td>Change Management - Standard Change Catalog</td>
<td>This plugin provides the change Management standard feature which allows Standard change templates to be proposed, approved, and published in the ServiceNow Service Catalog.</td>
<td>Active</td>
<td>true</td>
<td>com.snc.change_management, com.glideapp.servicecatalog</td>
</tr>
<tr>
<td>com.snc.change_management.state_model</td>
<td>Change Management - State Mode</td>
<td>This plugin provides the current Change Management state models for Standard, Normal and Emergency change types, originally released in the Geneva release.</td>
<td>Active</td>
<td>true</td>
<td>com.snc.change_management, com.snc.process_flow_formatter</td>
</tr>
<tr>
<td>com.glideapp.report.itsm.change.overview</td>
<td>Change Management Overview Homepage</td>
<td>Activates a Change Management Overview Dashboard in the Change Management application navigator.</td>
<td>Active</td>
<td>false</td>
<td>com.glideapp.report</td>
</tr>
<tr>
<td>com.glideapp.workflow_change_management</td>
<td>Change Management Workflows</td>
<td>This plugin activates the workflows which control the change processes associated with the Emergency, Normal, and Normal change types introduced in the Geneva release.</td>
<td>Active</td>
<td>true</td>
<td>com.glideapp.workflow</td>
</tr>
<tr>
<td>com.snc.change_request</td>
<td>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</td>
</tr>
<tr>
<td>com.snc.change_request_calendar</td>
<td>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>com.glide.channelproxy</td>
<td>Channel Proxy (New in London)</td>
<td></td>
<td>inActive</td>
<td>false</td>
<td>com.glide.external.app</td>
</tr>
<tr>
<td>Plugin ID</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>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.ing, com.glide.rest.service</td>
</tr>
<tr>
<td>Client Transaction Timings</td>
<td>com.glide.client.transaction.timings</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>
<tr>
<td>Cloud API</td>
<td>com.snc.cloud.api</td>
<td>Cloud API Framework.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.ui.ing, com.glide.ind, com.glide.rest.service</td>
</tr>
<tr>
<td>CMDB Dashboard</td>
<td>com.snc.cmdb.dashboard</td>
<td>Report overall CMDB and class level aggregated CI health.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.cmdb, com.snc.pi, com.glideapp.canvas</td>
</tr>
<tr>
<td>CMDB Group</td>
<td>com.snc.cmdb.group</td>
<td>Provides Configuration Item grouping capabilities.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.cmdb, com.snc.pi, com.glideapp.canvas</td>
</tr>
<tr>
<td>CMDB Group Dashboard</td>
<td>com.snc.cmdb.group.dashboard</td>
<td>Report the health of CIs in CMDB Groups, on a dashboard.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.cmdb, com.snc.pi, com.glideapp.canvas, com.snc.cmdb.group</td>
</tr>
<tr>
<td>CMDB Mainframe</td>
<td>com.snc.cmdb.mainframe</td>
<td>Configures plugins included in the Extended CMDB plugin, used for mainframe configuration items.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.cmdb</td>
</tr>
<tr>
<td>CMDB Radio Category</td>
<td>com.snc.cmdb.radio.category</td>
<td>Configures plugins included in the Extended CMDB plugin, used for radio configuration items.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.cmdb</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>CMDB Telecom Category</td>
<td>com.snc.cmdb</td>
<td>One of the plugins included in the Extended CMDB plugin, used for telecom configuration items.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.cmdb</td>
</tr>
<tr>
<td>CMDB Test Equipment</td>
<td>com.snc.cmdb</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>CMS User Interface - Service Management Core</td>
<td>com.snc.service_management.core.cms</td>
<td>All Content 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.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.cms, com.glide.cms.extensions, com.glide.db_images</td>
</tr>
<tr>
<td>Coaching Loops</td>
<td>com.snc.coaching_loops</td>
<td>Adds coaching functionality. This plugin facilitates the coaching of employees on their work through the use of coaching opportunities that can be conditionally configured.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.planned_task, com.glideapp.custom_charts</td>
</tr>
<tr>
<td>Code Search</td>
<td>com.glide.code_search</td>
<td>A configurable Code Search API.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Collaboration</td>
<td>com.glide.collaboration</td>
<td>Replaced by the Connect plugin.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.connect</td>
</tr>
<tr>
<td>Collision APIs</td>
<td>com.glide.collision_detector</td>
<td>APIs for detecting 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>Plugin ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
<td>---------------</td>
<td></td>
</tr>
<tr>
<td>Community</td>
<td>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.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.service-portal, com.sn_communities_global, com.snc.activity_subscription, com.snc.gamification, com.snc.cmdb.enterprise, com.glide.processor.ics, com.sn_kb_social_qa</td>
<td></td>
</tr>
<tr>
<td>Demo Data</td>
<td>Loads demo data for the community application.</td>
<td>Inactive</td>
<td>false</td>
<td>com.sn_communities_global, com.snc.cmdb.enterprise</td>
<td></td>
</tr>
<tr>
<td>Company Extension</td>
<td>Adds currency columns to the Company (core_company) table.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.currency</td>
<td></td>
</tr>
<tr>
<td>Configuration Compliance (New in London)</td>
<td>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.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.security_support.common</td>
<td></td>
</tr>
<tr>
<td>Configuration CMDB Management (CMDB Enterprise Edition)</td>
<td>Artisan assortment of modules for specialized configuration items, such as radio hardware, test equipment, and voice system hardware.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.cmdb</td>
<td></td>
</tr>
<tr>
<td>Configuration CMDB Management (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, com.sn_cmdb_content, com.snc.db.rotation, com.glide.util.list_v3.component</td>
<td></td>
</tr>
<tr>
<td>Configuration CMDB Management For Scoped Apps (CMDB)</td>
<td>Enables scoped apps access to Identification Engine APIs.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.cmdb.enterprise</td>
<td></td>
</tr>
<tr>
<td>Plugin ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------</td>
<td>----------------</td>
<td>-------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>cm.glide.connect.interaction-ui</td>
<td>User interface components to adapt Connect Support to use the interaction Support to use the interaction table as a source of truth.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.interaction, com.glide.graphql, com.glide.connect.support, com.glide.connect.ui_components</td>
<td></td>
</tr>
<tr>
<td>cm.glide.connect.interaction-ui</td>
<td>Scriptable APIs for Connect.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.service-portal, com.glide.connect, com.glide.connect.ui_components</td>
<td></td>
</tr>
<tr>
<td>cm.glide.connect.spoke-for-flow-designer</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>false</td>
<td>com.glide.connect.scriptable</td>
<td></td>
</tr>
<tr>
<td>cm.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>true</td>
<td>com.glide.connect.service-portal, com.glide.connect.support</td>
<td></td>
</tr>
<tr>
<td>cm.glide.connect.support-manager's-dashboard</td>
<td>Provides a homepage and all the configuration records required to analyze Connect Support in reporting.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.app.report</td>
<td></td>
</tr>
<tr>
<td>Plugin ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
<td>--------------</td>
<td></td>
</tr>
<tr>
<td>com.glide.connect.support.routing</td>
<td>Plugin that sets a processor for Routing Connect Support request to appropriate Chat Queue.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.matching_rule, com.glide.connect.support.routing</td>
<td></td>
</tr>
<tr>
<td>com.glide.service-portal.consumer-portal</td>
<td>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.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.service-portal.customer-service-base, com.glide.connect.anonymous-support</td>
<td></td>
</tr>
<tr>
<td>com.sn_content_automation</td>
<td>Content automation functionality.</td>
<td>Inactive</td>
<td>true</td>
<td>com.sn_content_delivery, com.glide.scope.access.restricted_caller</td>
<td></td>
</tr>
<tr>
<td>com.sn_content_delivery</td>
<td>Content Delivery</td>
<td>Inactive</td>
<td>true</td>
<td>com.glide.db_images, com.glide.scope.access.restricted_caller, com.glide.service-portal</td>
<td></td>
</tr>
<tr>
<td>com.glide.cms</td>
<td>Allows administrators to create custom, branded, web user interfaces on top of an existing ServiceNow instance.</td>
<td>Active</td>
<td>false</td>
<td>com.glideapp.home, com.glide.text_search, com.glide.db_images</td>
<td></td>
</tr>
<tr>
<td>com.glide.cms.types</td>
<td>An extension to Content Management that adds iFrames and Flash frames.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.cms.type.flash, com.glide.cms.type.iframe</td>
<td></td>
</tr>
<tr>
<td>com.glide.sorting</td>
<td>Support for drag-and-drop lists and ranking dialog. Context ranking allows a user to sort a collection of records independently of the attributes of those records. Context Ranking is activated automatically with the SDLC - Scrum Process Pack plugin.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.list_v2</td>
<td></td>
</tr>
<tr>
<td>Plugin ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------</td>
<td>----------------</td>
<td>-----------------------------------</td>
<td></td>
</tr>
<tr>
<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>com.snc.application.json_service, com.glide.db_view, com.glide.ui_page</td>
<td></td>
</tr>
<tr>
<td>com.snc.contextual_search</td>
<td>Displays related articles or service catalog items within a form or record producer.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.contextual_search, com.snc.application.json_service, com.snc.app_common.service_portal</td>
<td></td>
</tr>
<tr>
<td>com.snc.contextual_search.internal</td>
<td>Is a plugin component for Contextual Search.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.contextual_search.internal</td>
<td></td>
</tr>
<tr>
<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.role_management, com.glide.role_management.inh_count, com.glide.scripted_rest_services</td>
<td></td>
</tr>
<tr>
<td>com.glide.role_management.inh_count</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, com.glide.scripted_rest_services</td>
<td></td>
</tr>
<tr>
<td>com.glide.role_management.inh_count.rest_api</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, com.glide.scripted_rest_services</td>
<td></td>
</tr>
<tr>
<td>com.snc.contract_management</td>
<td>Provides the ability to manage all types of contracts.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.asset_management</td>
<td></td>
</tr>
<tr>
<td>com.glide.rest.cors</td>
<td>CORS support for REST API</td>
<td>Active</td>
<td>false</td>
<td>com.snc.asset_management</td>
<td></td>
</tr>
<tr>
<td>Plugin ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependency</td>
<td></td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------------</td>
<td>--------------------------</td>
<td></td>
</tr>
<tr>
<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>
<td></td>
</tr>
<tr>
<td>com.snc.problem_kb</td>
<td>Creates knowledge articles from a problem.</td>
<td>Active</td>
<td>false</td>
<td></td>
<td></td>
</tr>
<tr>
<td>com.glide.scope.access</td>
<td>Provides privilege capturing and enforcing cross-scope privileges used by Scoped Apps</td>
<td>Inactive</td>
<td>false</td>
<td></td>
<td></td>
</tr>
<tr>
<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>com.glide.ui.themes.core</td>
<td></td>
</tr>
<tr>
<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>
<td></td>
</tr>
<tr>
<td>com.glide.ui.themes.doctype</td>
<td>Provides UI themes.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.ui.themes.core</td>
<td></td>
</tr>
<tr>
<td>com.glideapp.servicecatalog.currency</td>
<td>Enables catalog to support fully localized currencies for item prices and options.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.currency</td>
<td></td>
</tr>
<tr>
<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>
<td></td>
</tr>
<tr>
<td>com.snc.customurl.internal</td>
<td>An internal plugin component to Scripted CustomURL APIs.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plugin ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
<td>--------------</td>
<td></td>
</tr>
<tr>
<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>
<td></td>
</tr>
<tr>
<td>com.snc.customer_service</td>
<td>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.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.asset_management, com.snc.state_flows, com.glide.connect.support, com.glide.connect.supportrouting, com.snc.assignment_workbench, com.snc.cs_base, com.snc.skills_management, com.snc.assessment_core, com.snc.process_flow, com.snc.task_relations, com.snc.task_activity, com.snc.matching_rule, com.snc.resolutionshaper, com.sn_openframe, com.sn_shn, com.snc.contextual_search, com.snc.cs_social</td>
<td></td>
</tr>
<tr>
<td>com.snc.customer_service_cti_demo</td>
<td>Provides demo data for the CTI Softphone application.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.customerservice, com.snc.cti</td>
<td></td>
</tr>
<tr>
<td>com.snc.customer_service_management_for_orders</td>
<td>Extends the Customer Service Management application to support order-related issues by integrating with order management systems to create and resolve customer requests.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.customerservice</td>
<td></td>
</tr>
<tr>
<td>Plugin ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
<td>---------------</td>
<td></td>
</tr>
<tr>
<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>
<td></td>
</tr>
<tr>
<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>
<td></td>
</tr>
<tr>
<td>com.snc.customer_service.spoke (New in London)</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>
<td></td>
</tr>
<tr>
<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>
<td></td>
</tr>
<tr>
<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.snc.db.replicate, com.glide.list_v2</td>
<td></td>
</tr>
<tr>
<td>Plugin Description</td>
<td>Plugin ID</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
<td>------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Data Lookup and Record Matching Support for Service Catalog</td>
<td>com.glide.data_lookup and record matching</td>
<td>Active</td>
<td>true</td>
<td>com.glideapp.servicecatalog.com.glide.data_lookup</td>
<td></td>
</tr>
<tr>
<td>Data Lookup and Record Matching Support</td>
<td>com.glide.data_lookup and record matching</td>
<td>Active</td>
<td>false</td>
<td>com.glideapp.servicecatalog.com.glide.data_lookup</td>
<td></td>
</tr>
<tr>
<td>Data Policy 2</td>
<td>com.glide.data_policy2</td>
<td>Active</td>
<td>false</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Structures</td>
<td>com.snc.datastructure</td>
<td>Active</td>
<td>false</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database Column Offrow Migration</td>
<td>com.glide.db.offrow_migration</td>
<td>Inactive</td>
<td>false</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database Rotation with Default Tables</td>
<td>com.snc.db.rotation</td>
<td>Active</td>
<td>false</td>
<td>com.snc.db.rotation</td>
<td></td>
</tr>
</tbody>
</table>

© 2019 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 ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.glide.db_audio</td>
<td>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>com.glide.db_images</td>
<td>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>com.glide.db_video</td>
<td>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>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>com.glide.ui.ng.datatables</td>
<td>DataTables 1.1.0 Components</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>com.snc.financial_management_cost_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_cost_model</td>
</tr>
<tr>
<td>com.sn_dd_user_admin</td>
<td>Delegated Dev User Administration.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<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>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>Plugin 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>
</tr>
<tr>
<td>Delete Recovery: Partial Undelete Support (New in London)</td>
<td>Extends the Delete Recovery plugin to support partially undeleting records from a transaction.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.delete_recovery.partial_undelete</td>
</tr>
<tr>
<td>Demand</td>
<td>com.snc.demand_management</td>
<td>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 Project Portfolio Suite with Financials plugin.</td>
<td>Inactive</td>
<td>true</td>
</tr>
<tr>
<td>Depreciation</td>
<td>com.snc.depreciation</td>
<td>Core depreciation capabilities.</td>
<td>Active</td>
<td>false</td>
</tr>
<tr>
<td>Designer</td>
<td>com.glide.ui.ng.dc</td>
<td>Provides common components required by designers such as the form designer and the quiz designer.</td>
<td>Active</td>
<td>false</td>
</tr>
<tr>
<td>Desired State Certification</td>
<td>com.snc.certification_desired_state</td>
<td>Evaluates records to see if they match a desired state, scheduled or on-demand.</td>
<td>Active</td>
<td>true</td>
</tr>
<tr>
<td>DHTMLX Gantt Library</td>
<td>com.snc.dhtmlx.gantt</td>
<td>DHTMLX Gantt library.</td>
<td>Inactive</td>
<td>false</td>
</tr>
<tr>
<td>DHTMLX Scheduler Library</td>
<td>com.snc.dhtmlx.scheduler</td>
<td>DHTMLX Scheduler library.</td>
<td>Active</td>
<td>false</td>
</tr>
<tr>
<td>Diagnostic Monitoring</td>
<td>com.glide.monitor.diagnostics</td>
<td>Provides advanced diagnostic monitoring of each node in a ServiceNow instance.</td>
<td>Active</td>
<td>false</td>
</tr>
<tr>
<td>Dictionary Overrides</td>
<td>com.glide.dictionary_override</td>
<td>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>
</tr>
<tr>
<td>Plugin Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
<td></td>
</tr>
<tr>
<td>--------------------</td>
<td>-------</td>
<td>----------------</td>
<td>---------------</td>
<td></td>
</tr>
<tr>
<td>Distribution Proxy</td>
<td>Active</td>
<td>false</td>
<td>com.glide.dist_download_proxy, com.snc.service_management.core</td>
<td></td>
</tr>
<tr>
<td>Dynamic Scheduling</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.matching_rule, com.glide.dist_download_proxy, com.glide.phone_number</td>
<td></td>
</tr>
<tr>
<td>E164 Compliant Phone Number</td>
<td>Active</td>
<td>true</td>
<td>com.glide.phone_number</td>
<td></td>
</tr>
<tr>
<td>Email - OAUTH support for IMAP and SMTP</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.email.oauth, com.glide.email_accounts, com.snc.platform.security.oauth</td>
<td></td>
</tr>
<tr>
<td>Email Access Restriction (New in London)</td>
<td>Active</td>
<td>false</td>
<td>com.glide.email_access_restriction, com.glide.email_accounts, com.snc.platform.security.oauth</td>
<td></td>
</tr>
<tr>
<td>Email Accounts</td>
<td>Active</td>
<td>false</td>
<td>com.glide.email_accounts, com.snc.platform.security.oauth</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-----------</td>
<td>----------------</td>
</tr>
<tr>
<td>Email Automatic User Creation</td>
<td>com.glide.email_auto</td>
<td>Sets glide.email.create_userid 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>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email Client Template</td>
<td>com.glide.email</td>
<td>Sets glide.email.create_userid 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>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email Digest</td>
<td>com.glide.email</td>
<td>Sets glide.email.create_userid 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>
</tr>
<tr>
<td>(New in London)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email Filters</td>
<td>com.glide.email</td>
<td>Sets glide.email.create_userid 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>Inactive</td>
<td>false</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email Notification Preview</td>
<td>com.glide.email</td>
<td>Sets glide.email.create_userid 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>Inactive</td>
<td>false</td>
</tr>
<tr>
<td>Preview Plugin</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email Notification</td>
<td>com.glide.email</td>
<td>Sets glide.email.create_userid 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>Inactive</td>
<td>false</td>
</tr>
<tr>
<td>Notification</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email Retention</td>
<td>com.glide.email</td>
<td>Sets glide.email.create_userid 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>Inactive</td>
<td>false</td>
</tr>
<tr>
<td>Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email Unsubscribe</td>
<td>com.glide.email</td>
<td>Sets glide.email.create_userid 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>Inactive</td>
<td>false</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plugin ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependence</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
<td>------------</td>
</tr>
<tr>
<td>com.glide.email_sms_separation</td>
<td>Separates 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.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.notification</td>
</tr>
<tr>
<td>com.glide.embedded_help</td>
<td>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.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.ui.hopscotch</td>
</tr>
<tr>
<td>com.sn_employee_document_management</td>
<td>Combined with other licensed applications, provides functionality to manage employee documents. Activates modules for Employee Documents in HR.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.documentviewer, com.glide.scope.access.restricted_caller</td>
</tr>
<tr>
<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>com.glide.encryption.core</td>
</tr>
<tr>
<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</td>
</tr>
<tr>
<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 Add Secure Info button that unhides these fields, and a Change Encryption 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>Plugin ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependences</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>com.snc.encrypted.scratchpad</td>
<td><strong>Encrypted Scratchpad</strong></td>
<td>Inactive</td>
<td>false</td>
<td>com.glideapp.workflow, com.glide.encryption</td>
</tr>
<tr>
<td>com.glideapp.email_engine_notifs</td>
<td><strong>Engine Based Notifications</strong></td>
<td>Active</td>
<td>false</td>
<td>com.glideapp.workflow, com.glide.encryption</td>
</tr>
<tr>
<td>com.glideapp.report.em</td>
<td><strong>Enhanced Web Service Provider - Common</strong></td>
<td>Active</td>
<td>false</td>
<td>com.glideapp.workflow, com.glide.encryption</td>
</tr>
<tr>
<td>com.snc.planned_task_v2</td>
<td><strong>Enterprise Release Management</strong></td>
<td>Inactive</td>
<td>true</td>
<td>com.glideapp.workflow, com.glide.encryption</td>
</tr>
<tr>
<td>com.glide.cms</td>
<td><strong>ESS Portal</strong></td>
<td>Active</td>
<td>true</td>
<td>com.glideapp.workflow, com.glide.encryption</td>
</tr>
<tr>
<td>com.glideapp.report, com.glideapp.itom.snac</td>
<td><strong>Event Management Overview Homepage</strong></td>
<td>Inactive</td>
<td>false</td>
<td>com.glideapp.workflow, com.glide.encryption</td>
</tr>
<tr>
<td>com.glide.stats</td>
<td><strong>Event stats</strong></td>
<td>Active</td>
<td>false</td>
<td>com.glideapp.workflow, com.glide.encryption</td>
</tr>
<tr>
<td>com.glideapp.execution_plan</td>
<td><strong>Execution Plan support for the service catalog</strong></td>
<td>Active</td>
<td>false</td>
<td>com.glideapp.workflow, com.glide.encryption</td>
</tr>
<tr>
<td>com.snc.expense_line</td>
<td><strong>Expense Line</strong></td>
<td>Active</td>
<td>false</td>
<td>com.glideapp.workflow, com.glide.encryption</td>
</tr>
<tr>
<td>Plugin ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencie(s)</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>com.snc.extended_cmdb</td>
<td>Provides specialized configuration items, such as radio hardware, test equipment, and voice system hardware.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.cmdb</td>
</tr>
<tr>
<td>com.snc.facilities_service_automation.move</td>
<td>Facilities Move Management. 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. <strong>Important:</strong> When licensed for Facilities Service Management and HR Service Delivery and a building map does not display in the HR Service Portal, try: Activating this plugin before, activating the Human Resources Scoped App: Lifecycle Events (com.sn_hr_lifecycle_events) plugin.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.service_management.core, com.snc.facilities_service_automation.fvw</td>
</tr>
<tr>
<td>Plugin 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>
</tr>
<tr>
<td>Facilities Service Management</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 plugin is required. Integration files installed when Facilities Visualization Workbench (com.snc.facilities_service_automation) 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</td>
</tr>
<tr>
<td>Facilities Service Management CMS Portal</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, com.snc.service_management</td>
</tr>
<tr>
<td>Plugin 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>
</tr>
<tr>
<td>Facilities Visualization Workbench</td>
<td>The Facilities Visualization Workbench provides map interaction built upon geoJSON file map sets. Integration files installed when Facilities Service Management (com.snc.facilities_service_automation) 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.glide.vars, com.glide.system_update_set</td>
</tr>
<tr>
<td>Field Normalization</td>
<td>Provides support for cleaning up messy data through normalization and transformation.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.field_normalization</td>
</tr>
<tr>
<td>Field Service - Questionnaire</td>
<td>Generate Questionnaires for Work Orders or Work Orders Tasks.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.wm_questionnaire</td>
</tr>
<tr>
<td>Field Service - 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.wo_signature_pad</td>
</tr>
<tr>
<td>Field Service Management</td>
<td>Provides support for scheduling and managing on-location work tasks.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.work_management</td>
</tr>
<tr>
<td>Field Service Management CMS Portal</td>
<td>Monitor and manage 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</td>
</tr>
<tr>
<td>Field Service Management Demo Data</td>
<td>Demonstrate 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.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.work_management</td>
</tr>
<tr>
<td>Plugin 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>
</tr>
<tr>
<td>Field Service Management Geolocation Demo Data</td>
<td>Enables geolocation capabilities for the Field Service Management application.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.work_management_geolocation.demo</td>
</tr>
<tr>
<td>Field Service Management Mobile</td>
<td>Enables the Field Service Management menu to the mobile user interface.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.work_management.mobile</td>
</tr>
<tr>
<td>Field Service Spoke (New in London)</td>
<td>Enables 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>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, com.snc.financial_planning_pmo</td>
</tr>
<tr>
<td>Field Service with Project Management Demo</td>
<td>Enables Field Service Management integration with the Project Management application.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.wm_ppm, com.snc.work_management, com.snc.customerservice.demo</td>
</tr>
<tr>
<td>Finance Service Management</td>
<td>Enables Finance Service Management 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</td>
</tr>
<tr>
<td>Finance Service Management CMS Portal</td>
<td>Enables Finance Service Automation and other service management applications from a single CMS page. 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, com.snc.service_management.cms_portal</td>
</tr>
<tr>
<td>Plugin 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>
</tr>
<tr>
<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>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>com.snc.financial_management_for_csm</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.snc.customerservice</td>
</tr>
<tr>
<td>Plugin 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>
</tr>
<tr>
<td>com.snc.financial_management_for_fsm</td>
<td>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.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.financial_management_for_fsm, com.snc.work_management, com.snc.pa, com.snc.pa.fm.fsm</td>
</tr>
<tr>
<td>com.snc.financial_planning_default_definition</td>
<td>Provides a configured 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_default_definition</td>
</tr>
<tr>
<td>com.snc.fiscal_calendar</td>
<td>Enables you 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.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.dynamic_operands.datetime</td>
</tr>
<tr>
<td>com.snc.fixed_asset</td>
<td>Provides fixed asset tracking</td>
<td>Active</td>
<td>false</td>
<td>com.glide.hub.designer_backend.suite</td>
</tr>
<tr>
<td>Plugin ID</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
</tr>
<tr>
<td>-----------</td>
<td>----</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
</tr>
<tr>
<td>Flow Designer Action Step - CORE (New in London)</td>
<td>com.glide.hub.action_step.core</td>
<td>Action Step - Core operations on GlideRecord.</td>
<td>Active</td>
<td>false</td>
</tr>
<tr>
<td>Plugin Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependence</td>
<td></td>
</tr>
<tr>
<td>--------------------</td>
<td>-------</td>
<td>----------------</td>
<td>------------</td>
<td></td>
</tr>
<tr>
<td>Action Step - CRUD operations on GlideRecord.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.hub.action_step.template</td>
<td></td>
</tr>
<tr>
<td>Action Step - Email.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.email.service, com.glide.hub.action_step.template</td>
<td></td>
</tr>
<tr>
<td>Action Step - Log.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.hub.action_step.template</td>
<td></td>
</tr>
<tr>
<td>Action Step - Notification.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.notification, com.glide.hub.action_step.template</td>
<td></td>
</tr>
<tr>
<td>Action Step - Script.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.hub.action_step.template</td>
<td></td>
</tr>
<tr>
<td>Plugin ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependences</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Flow Designer Action Step Template (New in London)</td>
<td>Action Step Template</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Flow Designer Action Trigger (New in London)</td>
<td>Action triggers that map a Trigger (Record, Email, REST) to an Action</td>
<td>Active</td>
<td>false</td>
<td>com.glide.hub.flow_trigger</td>
</tr>
<tr>
<td>Flow Designer Scriptable Plan Runner APIs</td>
<td>Scriptable Plan Runner APIs</td>
<td>Active</td>
<td>false</td>
<td>com.glide.hub.flow_engine</td>
</tr>
<tr>
<td>Plugin 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>
</tr>
<tr>
<td>com.glide.hub.action_type.system</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>
</tbody>
</table>
| com.glide.ui.personalization | Enables users to personalize the layout for any form view. | Active | false | com.glide.ui.doctype 
| com.snc.fullcalendar | Fullcalendar library v2.5.0. | Inactive | false | 
| com.snc.geolocation | 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. | Inactive | false | 
| com.glide.metadata | Glide metadata support. | Active | false | com.snc.metadata, com.snc.metadata_tree 
| com.glide.metadata.delete | Glide metadata delete support. | Active | false | 
| com.snc.global.application.file.management | Utilities and components for managing application files in the global scope. | Active | false | com.glide.scripted_rest_service, com.glide.ui.service 
| com.glide.app.google_maps_plugin | Glide Maps plugin of Google Maps within the product as map pages. | Active | false | com.glide.ui.service, com.glide.rest.service 
| com.snc.contextual.search.schema | GraphQL schema for contextual search services | true | false | com.glide.graphql 

© 2019 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 ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependence</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.snc.knowledge_graphql</td>
<td>Provides GraphQL schema for contextual search sources like Knowledge and Social Q&amp;A</td>
<td>true</td>
<td>false</td>
<td>com.snc.contextual_search.portfolio_management</td>
</tr>
<tr>
<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>com.sn_comp_ucf</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>
<tr>
<td>com.sn_grc_pa</td>
<td>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.</td>
<td>Inactive</td>
<td>false</td>
<td>com.sn_grc</td>
</tr>
<tr>
<td>Plugin 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>
</tr>
<tr>
<td>GRC: Policy and Compliance Management</td>
<td>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.</td>
<td>Inactive</td>
<td>true</td>
<td>com.sn_grc, com.snc.comp_attest</td>
</tr>
<tr>
<td>GRC: Risk Management</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>GRC: SIG Questionnaire Integration</td>
<td>The GRC: SIG Questionnaire Integration plugin installs the Shared Assessments Standardized Information Gathering (SIG) questionnaire for use with the GRC: Vendor Risk Management application.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.assessment_core, com.vnvriskasmt, com.snc.sigasmt_core, com.snc.document_management</td>
</tr>
<tr>
<td>GRC: Vendor Risk Management</td>
<td>The GRC: Vendor Risk Management application allows risk management stakeholders to identify, assess, and manage risk across the vendor ecosystem.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc_comp_asmt, com.snc.vendor_core, com.snc_grc, com.snc.vriskasmt_designer, com.snc.vendor_portal</td>
</tr>
<tr>
<td>Plugin 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>
</tr>
<tr>
<td>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 Setup for CMDB</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, com.snc.cmdb</td>
</tr>
<tr>
<td>Guided Setup Framework</td>
<td>Provides customers with visual guidance to configure ServiceNow applications.</td>
<td>Active</td>
<td>false</td>
<td>com.glideapp.ui_components, com.glide.scripted_rest_services, com.glide.embedded_help, com.glide.scoped_analytics</td>
</tr>
<tr>
<td>Guided Tour Designer</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>com.glide.ui.hopscotch, com.glide.embedded_help</td>
</tr>
<tr>
<td>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, com.glide.embedded_help</td>
</tr>
<tr>
<td>High Security Settings</td>
<td>Select 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>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
</tr>
<tr>
<td>History Sets</td>
<td>com.glide.hist</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>
</tr>
<tr>
<td>History Walker</td>
<td>com.glide.hist</td>
<td>Provides script access to History Walker</td>
<td>Active</td>
<td>false</td>
</tr>
<tr>
<td>Homesplash Page</td>
<td>com.glideapp.home</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>
</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>
</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>
</tr>
<tr>
<td>Plugin ID</td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human Resources Scoped App: Core</td>
<td>Provides case and change management for HR. Ensure that you do not have the Human Resources Application: Core plugin activated. Duplication of functionality is possible. Activation of this plugin on production instances requires a separate license. Contact ServiceNow for details.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human Resources Scoped App: Integrations</td>
<td>Activates 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></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human Resources Scoped App: Lifecycle Events</td>
<td>Activates the Lifecycle Event module for HR. Combined with other licensed applications, provides a full-service, onboarding experience for new hires and employees managing the process.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Important:**

To use the Floor Plan Viewer in the HR Service Portal, activate the Facilities Move Management (com.snc.facilities_service_automation.move) plugin before activating this plugin.
<table>
<thead>
<tr>
<th>Plugin ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.sn.hr.scoped</td>
<td>Human Resources Scoped App: Security</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.service-</td>
</tr>
<tr>
<td></td>
<td>Activation</td>
<td></td>
<td></td>
<td>portal</td>
</tr>
<tr>
<td></td>
<td>Requires activation of this plugin on production instances requires</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a separate license. Contact ServiceNow for details.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Human Resources Scoped App: Core plugin requires this plugin.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Provides a single place for employees to quickly and easily get all the HR</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>services they need.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>com.snc.i18n.br.</td>
<td>Brazilian Portuguese Translations</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td></td>
<td>An Internationalization plugin for language internationalization. Provides</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Brazilian Portuguese.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>com.snc.i18n.cs.</td>
<td>Czech Translations</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td></td>
<td>An Internationalization plugin for language internationalization. Provides</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Czech.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>com.snc.i18n.nl.</td>
<td>Dutch Translations</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td></td>
<td>An Internationalization plugin for language internationalization. Provides</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dutch.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>com.snc.i18n.fi.</td>
<td>Finnish Translations</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td></td>
<td>An Internationalization plugin for language internationalization. Provides</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Finnish.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>com.snc.i18n.fr.</td>
<td>French Translations</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td></td>
<td>An Internationalization plugin for language internationalization. Provides</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>French - Canadian.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>com.snc.i18n.fr.</td>
<td>French Translations</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td></td>
<td>An Internationalization plugin for language internationalization. Provides</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>French.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>com.snc.i18n.de.</td>
<td>German Translations</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td></td>
<td>An Internationalization plugin for language internationalization. Provides</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>German.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>com.snc.i18n.he.</td>
<td>Hebrew Translations</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td></td>
<td>An Internationalization plugin for language internationalization. Provides</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hebrew.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plugin 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>
</tr>
<tr>
<td>I18n: Hungarian Translations</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>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, com.glideapp.knowledge3, com.glide.i18n</td>
</tr>
<tr>
<td>I18n: Translation helper</td>
<td>Translation helper 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>An Internationalization plugin for language internationalization. Provides Italian.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td>I18n: Japanese Translations</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>Knowledge Management Internationalization Plugin v2</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, com.glide.i18n</td>
</tr>
<tr>
<td>I18n: Korean Translations</td>
<td>Korean Translations</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td>I18n: Polish Translations</td>
<td>Polish 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>Portuguese Internationalization plugin for language internationalization. Provides Portuguese.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td>Plugin 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>
</tr>
<tr>
<td>com.snc.i18n.ru</td>
<td>Russian Internationalization plugin for language internationalization. Provides Russian.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td>com.snc.i18n.ce</td>
<td>Simplified Chinese Internationalization plugin for language internationalization. Provides Simplified Chinese.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td>com.snc.i18n.sv</td>
<td>Spanish Internationalization plugin for language internationalization. Provides Spanish.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td>com.snc.i18n.th</td>
<td>Thai Internationalization plugin for language internationalization. Provides Thai.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td>com.snc.i18n.ta</td>
<td>Traditional Chinese Internationalization plugin for language internationalization. Provides Traditional Chinese.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td>com.snc.i18n.tr</td>
<td>Turkish Internationalization plugin for language internationalization. Provides Turkish.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.i18n</td>
</tr>
<tr>
<td>com.snc.incident</td>
<td>Provides base functionality for Incident Management.</td>
<td>Active</td>
<td>true</td>
<td>com.glideapp.report.itsm</td>
</tr>
<tr>
<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.glideapp.live_feed</td>
</tr>
<tr>
<td>com.snc.best_practice.london</td>
<td>Overrides dictionary for state field on incident table and new properties are added to Incident.</td>
<td>Active</td>
<td>false</td>
<td>None</td>
</tr>
<tr>
<td>Plugin 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>
</tr>
<tr>
<td>Incident Management - Major Incident Management</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.update_data, com.snc.task_outage</td>
</tr>
<tr>
<td>Incident Management 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>Provides incident overview functionality to Incident Management.</td>
<td>Active</td>
<td>false</td>
<td>com.glideapp.report</td>
</tr>
<tr>
<td>Incident Resolution Fields</td>
<td>Adds Resolved and Resolved by fields to the Incident table, similar to Closed and Closed by, 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>Incident Updates Plugin - Includes any updates to the Incident Base Plugin.</td>
<td>Active</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>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>Insert Multiple Web Service</td>
<td>Enables multiple inserts for the Direct SOAP API.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Instance Security Dashboard (PA) (New in London)</td>
<td>Instance Security Dashboard using Performance Analytics. To access the complete set of functionalities for this dashboard, activate the Performance Analytics - Instance Security Dashboard plugin.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Integration - Common Components</td>
<td>Provides common scripts for integrations.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.system_import, com.glide.web_service_provider, com.glide.system_properties</td>
</tr>
<tr>
<td>Plugin 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>
</tr>
<tr>
<td>Integration - JDBC</td>
<td>Provides integration through JDBC.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.web_service_application, com.glideapp.agent, com.snc.integration.common</td>
</tr>
<tr>
<td>Integration - Microsoft SCCM 2016</td>
<td>Integration 2016 with Microsoft SCCM.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.integration.jdbc, com.snc.ci.identification</td>
</tr>
<tr>
<td>Integration - Microsoft SMS / SCCM 2.0 (Deprecated)</td>
<td>Legacy version 2.0 integration with Microsoft SMS/SCCM. Replaced by Integration - Microsoft SCCM 2007.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.integration.jdbc</td>
</tr>
<tr>
<td>Integration - Multifactor Authentication</td>
<td>This plugin installs Multifactor authentication on the instance.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Integration - Multiple Provider Single Sign-On Enhanced UI</td>
<td>Provides SSO functionality with multiple providers.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.ui.ng.guided_flow, com.snc.integration.sso.multi.ui</td>
</tr>
<tr>
<td>Plugin 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>
</tr>
<tr>
<td>Integration - Multiple Provider Single Sign-On 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>com.snc.integration.com.snc.integration.sso.multi.installer</td>
</tr>
<tr>
<td>Integration - OpenID SSO (Deprecated)</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.com.snc.integration.sso.openid</td>
</tr>
<tr>
<td>Integrations - External Authentication Framework</td>
<td>External.app</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.external.app</td>
</tr>
</tbody>
</table>

© 2019 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>Interactive Analysis</td>
<td>com.glideapp.interactive_analysis</td>
<td>Interactive Analysis</td>
<td>Active</td>
<td>false</td>
<td>com.glideapp.home, pub, com.glide.ui, amb, com.glide.ui.form_elements</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>com.glideapp.home, pub, com.glide.ui, amb, com.glide.ui.form_elements</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>com.glideapp.servicecatalog</td>
</tr>
<tr>
<td>ITOM Guided Setup</td>
<td>com.snc.guided_setup_itom_metadata</td>
<td>ITOM Guided Setup Metadata.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.guided_setup</td>
</tr>
<tr>
<td>ITSM and PA Demo Data</td>
<td>com.snc.itsm_pa.demo</td>
<td>Demo data for Incident, Problem, Change, Task SLAs, Business Services, Service Offering, Service Commitments, and Performance Analytics.</td>
<td>Inactive</td>
<td>true</td>
<td>com.glideapp.servicecatalog</td>
</tr>
<tr>
<td>ITSM Guided Setup</td>
<td>com.snc.guided_setup_itsm</td>
<td>Contains metadata for ITSM Guided Setup. This plugin is for ServiceNow internal usage only.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.guided_setup</td>
</tr>
<tr>
<td>ITSM Spoke (New in London)</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>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, com.glide.snc_code_editor</td>
</tr>
<tr>
<td>JSDebugger</td>
<td>com.glide.js-debugger</td>
<td>ServiceNow server-side scripts debugger.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.js-debugger-api</td>
</tr>
<tr>
<td>Plugin ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependence</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
<td>------------</td>
<td></td>
</tr>
<tr>
<td>JSON Service request/response model</td>
<td>Adds 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>
<td></td>
</tr>
<tr>
<td>Knowledge Document</td>
<td>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.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.document_management, com.snc.knowledge_document</td>
<td></td>
</tr>
<tr>
<td>Knowledge Management - External Content Integration (New in London)</td>
<td>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.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.core.automation.connection_credential, com.snc.knowledge3, com.snc.knowledge_advanced.installer, com.glide.service-portal.esm</td>
<td></td>
</tr>
<tr>
<td>Knowledge Management - Service portal</td>
<td>Adds knowledge management features on the service portal.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.service-portal.esm, com.snc.knowledge3</td>
<td></td>
</tr>
<tr>
<td>Knowledge Management Advanced</td>
<td>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>
<td></td>
</tr>
<tr>
<td>Plugin ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependency</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>Knowledge Management Advanced Installer</td>
<td>Information about the Knowledge Management Advanced Installer plugin, which installs the Knowledge Advanced plugin. When you activate or 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.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.knowledge_advanced.installer</td>
<td></td>
</tr>
<tr>
<td>Knowledge Management Wiki Support</td>
<td>Activate this plugin to enable support for Wiki type Knowledge articles.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.wiki, com.glideapp.knowledge2, com.glideapp.knowledge2.wiki</td>
<td></td>
</tr>
<tr>
<td>Knowledge Overview Homepage</td>
<td>Knowledge Overview Homepage.</td>
<td>Active</td>
<td>false</td>
<td>com.glideapp.report.knowledgeoverview</td>
<td></td>
</tr>
<tr>
<td>Knowledge 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.snc.kb_product_entitlements</td>
<td></td>
</tr>
<tr>
<td>Plugin ID</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</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, com.snc.service_management.cms</td>
</tr>
<tr>
<td>Legal Service Management CMS Portal</td>
<td>com.snc.legal_service_automation.cms</td>
<td>Lets you launch Legal Service Automation and other service management applications from a single CMS page. 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.legal_service_automation, com.snc.service_management</td>
</tr>
<tr>
<td>Legal Service Management Mobile</td>
<td>com.snc.legal_service_automation_m</td>
<td>Manages Legal Service Management mobile components.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.legal_service_automation, com.snc.service_management_m</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>Create deep links on any form to payroll, social media, or to products to fulfill computer or software requests. Generate URLs to manage content, knowledge articles, and catalogs.</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, com.glide.ui.list_edit_with_form, com.glide.db_context_menu</td>
</tr>
<tr>
<td>Live Feed</td>
<td>com.glideapp.live_feed</td>
<td>Provides an updated application to post and share content in a ServiceNow instance.</td>
<td>Active</td>
<td>true</td>
<td>com.glideapp.live_feed, com.glideapp.ui_components</td>
</tr>
<tr>
<td>Plugin ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
<td>--------------</td>
<td></td>
</tr>
<tr>
<td>Live Feed</td>
<td>Provides a place to post and share content in a ServiceNow instance.</td>
<td>Active</td>
<td>true</td>
<td>com.glide.custom_web_service, com.glideapp.live_feed_common, com.glide.notification</td>
<td></td>
</tr>
<tr>
<td>Live Feed Document</td>
<td>Enables you to manage your task conversations and comments from My Feed or a document group.</td>
<td>Active</td>
<td>false</td>
<td>com.glideapp.live_feed</td>
<td></td>
</tr>
<tr>
<td>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, com.glide.ui.doctype, com.glide.ui.ng</td>
<td></td>
</tr>
<tr>
<td>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, com.snc.cmdb</td>
<td></td>
</tr>
<tr>
<td>Major Issue Management (New in London)</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, com.sn_publications, com.snc.task_communication_management</td>
<td></td>
</tr>
<tr>
<td>Managed Documents</td>
<td>A 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>
<td></td>
</tr>
<tr>
<td>Plugin ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
<td>---------------</td>
<td></td>
</tr>
<tr>
<td>com.snc.marketing_service_management</td>
<td>Marketing Service Management</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.marketing_service_management</td>
<td></td>
</tr>
<tr>
<td>com.snc.marketing_service_management.cms</td>
<td>Marketing Service Automation and other service management applications from a single CMS page. Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.marketing_service_management.cms, com.snc.service_management.core.cms</td>
<td></td>
</tr>
<tr>
<td>com.glide.ui.merge_tool</td>
<td>Merge Tool</td>
<td>Active</td>
<td>false</td>
<td>com.glide.ui.angular, com.glide.snc_code_editor</td>
<td></td>
</tr>
<tr>
<td>com.glide.system_update_set</td>
<td>Metadata Source Control</td>
<td>Active</td>
<td>false</td>
<td>com.glide.system_update_set</td>
<td></td>
</tr>
<tr>
<td>com.snc.metadata_tree</td>
<td>Metadata Tree</td>
<td>Active</td>
<td>false</td>
<td>com.snc.apps_file</td>
<td></td>
</tr>
<tr>
<td>com.snc.threat.metadefender</td>
<td>Metadefender Integration</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.threat.intelligence</td>
<td></td>
</tr>
<tr>
<td>com.glide.metrics</td>
<td>Metric Definition</td>
<td>Active</td>
<td>true</td>
<td>com.glide.schedules</td>
<td></td>
</tr>
<tr>
<td>com.glide.ui.mergetool</td>
<td>Merge Tool</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.highcharts, com.glide.hub.flow_trigger</td>
<td></td>
</tr>
</tbody>
</table>

© 2019 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 ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft AD Spoke for IntegrationHub (New in London)</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, com.glide.hub.action_step.powershell</td>
</tr>
<tr>
<td>Microsoft Azure AD Spoke for IntegrationHub (New in London)</td>
<td>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.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.hub.designer_backend.model, com.glide.hub.action_step.rest</td>
</tr>
<tr>
<td>MID Server</td>
<td>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 (New in London)</td>
<td>Distributed 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>Mobile Device ITIL and Service Management</td>
<td>Applications and modules for ITIL and Service Management.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.labels, com.glide.mobile</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
<td>----------------</td>
</tr>
<tr>
<td>Mode 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>
</tr>
<tr>
<td>Mutex stats</td>
<td>com.glide.stats</td>
<td>Mutex stats.</td>
<td>Active</td>
<td>false</td>
</tr>
<tr>
<td>My Assets</td>
<td>com.snc.asset</td>
<td>Provides users with self-service access to their own assets, contracts, and requests.</td>
<td>Active</td>
<td>false</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>
</tr>
<tr>
<td>Plugin 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>
</tr>
<tr>
<td>NG shared components</td>
<td>Provides libraries and services common to plugins using Angular.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.ui.angular, com.glide.ui.angularui, com.glide.ui.ng.amb</td>
</tr>
<tr>
<td>Normalization Data Services 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></td>
<td>Active</td>
<td>false</td>
<td>com.snc.guided_setup</td>
</tr>
<tr>
<td>Notification Preference Service</td>
<td>Define a 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>Define a javascript 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, com.glide.notification.system.pushaddon, com.glide.notification.preference.service</td>
</tr>
<tr>
<td>Notification System Push Addon</td>
<td>Add support for push notifications to the notification system.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.notification, com.glide.push</td>
</tr>
<tr>
<td>Notify</td>
<td>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.</td>
<td>Inactive</td>
<td>true</td>
<td>com.glide.phone_number, com.snc.notify.twilio</td>
</tr>
<tr>
<td>Notify - Twilio Driver</td>
<td>Provides Notify support for Twilio. Requires a separate contract with Twilio for SMS/Voice capabilities.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.phone_number</td>
</tr>
<tr>
<td>OAuth 2.0</td>
<td>Adds support for SAML authentication of OAuth 2.0 to support token granting and authentication.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.certificate, com.snc.platform.security</td>
</tr>
<tr>
<td>Plugin 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>
</tr>
<tr>
<td>OAuth 2.0 legacy (Do not activate. Use 'OAuth 2.0')</td>
<td>Legacy implementation of OAuth 2.0. Install com.snc.platform.security.oauth instead.</td>
<td>Active</td>
<td>false</td>
<td>oauth</td>
</tr>
<tr>
<td>ODBC Commons</td>
<td></td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>On-Call Scheduling</td>
<td>Provisions 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, com.glide.notification, com.glide.ui.ng, com.snc.app.calendar, com.snc.fullcalendar</td>
</tr>
<tr>
<td>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>Ordered Email Processing</td>
<td>Allows inbound processing actions to be ordered, and programmatically stop processing.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Organization Extension</td>
<td>Provides Enterprise Strategy and Business Unit strategy entities.</td>
<td>Active</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>Organization Management</td>
<td></td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Outbound Email Notifications</td>
<td></td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Outbound HTTP Log</td>
<td></td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
</tbody>
</table>

© 2019 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 ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<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>com.glide.ui.overview_help</td>
<td>Framework for Overview pages.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.ui.angular</td>
</tr>
<tr>
<td>com.glide.script.packages_call_removal</td>
<td>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>com.glideapp.password_reset</td>
<td>Provides the ability to create self-service and service desk password reset processes for a ServiceNow instance.</td>
<td>Active</td>
<td>true</td>
<td>com.snc.process_flow_formatter, com.glide.notification, com.glide.usageanalytics</td>
</tr>
<tr>
<td>com.glideapp.password_reset_desktop</td>
<td>Password Reset Windows integration.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<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>com.snc.performance_analytics</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, com.glideapp.report, com.glideapp.home.publishers, com.snc.core.automation, com.glide.usageanalytics</td>
</tr>
<tr>
<td>Plugin 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>
</tr>
</tbody>
</table>
| Performance Analytics - Administrator Console | A single console where you can:  
· Explore and manage out-of-the-box content and Performance Analytics widgets and dashboards  
· Diagnose and resolve configuration errors  
· View usage analytics  
· Modify advanced configuration settings  
| Performance Analytics - Configuration Generator | A configuration generator for creating a set of Performance Analytics indicators, breakdowns, dashboards, and widgets based on the task-derived table. | Inactive   | false          | com.snc.pa.configurationgenerator                                              |
| Performance Analytics - Content Pack - Application Portfolio Management (New in London) | Application Portfolio Management dashboards developed using Performance analytics premium. | Inactive   | true           | com.snc.apm, com.snc.pa                                                      |
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_management                         |
<table>
<thead>
<tr>
<th>Plugin ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.snc.pa.apm.com.snc.pa.apm.problem</td>
<td>Performance 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.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.apm, com.snc.pa, com.snc.pa.problem</td>
</tr>
<tr>
<td>com.snc.pa.change.com.snc.pa.change</td>
<td>Performance Analytics content pack for Change Management out-of-the-box KPIs. 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.glideapp.report.itsm.change.overview</td>
</tr>
<tr>
<td>com.snc.pa.cmp.com.snc.pa.cmp</td>
<td>Performance Analytics content pack Cloud Management out-of-the-box KPIs. 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.runbook_automation.virtualization</td>
</tr>
<tr>
<td>com.snc.pa.cmdb.com.snc.pa.cmdb</td>
<td>Performance Analytics content pack Configuration Management (CMDB) out-of-the-box KPIs. 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.cmdb, com.snc.pa.change</td>
</tr>
<tr>
<td>com.snc.pa.communities.com.snc.pa.communities</td>
<td>Performance Analytics content pack Communities out-of-the-box KPIs. 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.sn_communities</td>
</tr>
<tr>
<td>Plugin 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>
</tr>
<tr>
<td>com.snc.pa.customer_service</td>
<td>Performance Analytics content pack Customer Service out-of-the-box KPIs. 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.glideapp.report.customer service, com.sn_customerservice, com.sn_customerservice_pa</td>
</tr>
<tr>
<td>com.snc.pa.discovery</td>
<td>Performance Analytics content pack for Discovery out-of-the-box KPIs. 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.pa.cmdb, com.snc.discovery</td>
</tr>
<tr>
<td>com.snc.pa.em</td>
<td>Performance Analytics content pack for Event Management core out-of-the-box KPIs. 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.glideapp.itom.snac, com.glideapp.report.em</td>
</tr>
<tr>
<td>com.snc.work_management_pa</td>
<td>Performance Analytics content pack 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, com.snc.work_management</td>
</tr>
<tr>
<td>com.snc.pa.fm</td>
<td>Performance Analytics content pack Financial Management out-of-the-box KPIs. 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>Plugin 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>
</tr>
<tr>
<td>com.snc.pa.fm.com.snc.pa.fm</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>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>com.sn_audit_pa.com.sn_audit</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>Plugin ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependence</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
<td>------------</td>
</tr>
<tr>
<td>Performance Analytics</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</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>Performance Analytics</td>
<td>Provides Performance Analytics reports and dashboard for the scoped HR application Employee Document Management.</td>
<td>Inactive</td>
<td>false</td>
<td>com.sn_employee_document_management, com.sn_hr_core</td>
</tr>
<tr>
<td>Plugin 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>
</tr>
<tr>
<td>Performance Analytics - Content Pack - Human Resources Lifecycle Events Scoped App (New in London)</td>
<td>Provides Performance Analytics reports for Scoped HR Lifecycle Events. 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>Performance Analytics - Content Pack - Human Resources Scoped App</td>
<td>Provides Performance Analytics reports for Scoped HR. Activation of this plugin on production requires 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>Performance Analytics content pack for Incident SLA Management out-of-the-box KPIs. 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.sla</td>
</tr>
<tr>
<td>Plugin 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>
</tr>
<tr>
<td>com.snc.pa.knowledge_v2</td>
<td>Performance Analytics content pack for Knowledge Management out-of-the-box KPIs. 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.knowledge3, com.glideapp.report.knowl3, com.glideapp.report.knowl4</td>
</tr>
<tr>
<td>Plugin 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>
</tr>
<tr>
<td>Performance Analytics - Content Pack - Request Management (Requested Item)</td>
<td>Performance Analytics content pack for Request Management out-of-the-box KPIs 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>Performance Analytics content pack for Request Management out-of-the-box KPIs 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>Performance Analytics - Content Pack - Service Mapping (New in London)</td>
<td>Performance Analytics content pack for Service Mapping out-of-the-box Dashboard and KPIs. 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.pa.cmdb</td>
</tr>
<tr>
<td>Performance Analytics - Content Pack for ITSM</td>
<td>installing this plugin installs content packs for Incident, Problem, Change, Incident SLA, Knowledge, and Requested Items for Performance Analytics.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.pa.change, com.snc.pa.problem, com.snc.pa.request, com.snc.pa.request2, com.snc.pa.knowledge, com.snc.pa.sla</td>
</tr>
<tr>
<td>Plugin 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>
</tr>
<tr>
<td>com.snc.pa.change.context_sensitive_analytics</td>
<td>Provides additional ability to open PA context sensitive PA dashboards in change request form based on UI actions.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.pa, com.snc.pa.change</td>
</tr>
<tr>
<td>com.snc.pa.chat.context_sensitive_analytics</td>
<td>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.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.pa, com.snc.pa.chat</td>
</tr>
<tr>
<td>com.snc.pa.cs.context_sensitive_analytics</td>
<td>Performance Analytics adding ability to open PA context-sensitive dashboards in customer service form based on UI actions.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.pa, com.snc.pa.customer_service, com.sn_customerservice, com.snc.pa.customer_service</td>
</tr>
<tr>
<td>com.snc.pa.incident.context_sensitive_analytics</td>
<td>Performance Analytics adding ability to open PA context-sensitive dashboards in incident form based on UI actions.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.pa</td>
</tr>
<tr>
<td>com.snc.pa.problem.context_sensitive_analytics</td>
<td>Performance Analytics adding ability to open PA context sensitive PA dashboards in problem form based on UI actions.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.pa, com.snc.pa.problem</td>
</tr>
<tr>
<td>Plugin 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>
</tr>
<tr>
<td>com.snc.pa.dc</td>
<td>Data Collector for Performance Analytics. Deprecated. Use plugin Performance Analytics instead</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>com.snc.pa.diagnostics</td>
<td>Enables users to run diagnostics on Performance Analytics records and related applications.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.pa</td>
</tr>
<tr>
<td>com.snc.pa.linkedin</td>
<td>Automatically imports LinkedIn data historically and daily.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.pa</td>
</tr>
<tr>
<td>com.snc.pa.stock</td>
<td>Automatically imports stock quotes data historically and daily.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.pa</td>
</tr>
<tr>
<td>com.snc.pa.twitter</td>
<td>Automatically imports Twitter data historically and daily.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.pa</td>
</tr>
<tr>
<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>
<tr>
<td>Plugin 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>
</tr>
<tr>
<td>Performance Analytics - 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_l1) and Scores Level 2 (pa_scores_l2). 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.scores_migration</td>
</tr>
<tr>
<td>Performance Analytics - 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.spotlight</td>
</tr>
<tr>
<td>Performance Analytics - Spotlight - change spotlight content pack</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.spotlight.change</td>
</tr>
<tr>
<td>Performance Analytics - Spotlight - Incident Spotlight content pack</td>
<td>Enables records to be ranked by multiple weighted criteria. To provide optimal performance, the Scores (pa_scores) table is being migrated to Scores Level 1 (pa_scores_l1) and Scores Level 2 (pa_scores_l2). During migration you cannot collect, modify, or delete scores. Scheduled data collection and cleanup jobs will not run during migration.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.pa.spotlight.incident</td>
</tr>
<tr>
<td>Performance Analytics - Spotlight - Problem Spotlight content pack</td>
<td>Enables records to be ranked by multiple weighted criteria. To provide optimal performance, the Scores (pa_scores) table is being migrated to Scores Level 1 (pa_scores_l1) and Scores Level 2 (pa_scores_l2). During migration you cannot collect, modify, or delete scores. Scheduled data collection and cleanup jobs will not run during migration.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.pa.spotlight.problem</td>
</tr>
<tr>
<td>Plugin 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>
</tr>
<tr>
<td>com.snc.pa.spotlight.request.content.pack</td>
<td>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, com.snc.pa.request2</td>
</tr>
<tr>
<td>com.snc.pa.sp.widget</td>
<td>Support for PA widgets in the Service Portal. A number of JavaScript and CSS libraries are included to be able to run PA widgets independently in the Service Portal.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.service-portal</td>
</tr>
<tr>
<td>com.snc.pa.incident.mim</td>
<td>Provides out-of-the-box KPIs and dashboards 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>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>
| com.snc.pa.premium | Enables the functionality you are entitled to with a subscription to Performance Analytics across all other 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 ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance Analytics and Reporting - Service Portal Widgets (New in London)</td>
<td>Support for PA widgets in the Service Portal. A number of JavaScript and CSS libraries are included to be able to run PA widgets independently in the Service Portal.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.service-portal</td>
</tr>
<tr>
<td>Performance Analytics Premium for APM</td>
<td>Enables the functionality you are entitled to with a subscription to 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</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.pa</td>
</tr>
<tr>
<td>Performance Analytics Premium for Business Management</td>
<td>Enables the functionality you are entitled to with a subscription to 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</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.pa</td>
</tr>
<tr>
<td>Plugin ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependency</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
<td>--------------------------</td>
</tr>
</tbody>
</table>
| Performance Analytics Premium for Cloud Control Center | Enables the functionality you are entitled to with a subscription to 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.premium.ccc  |
| Performance Analytics Premium for Customer Service | Enables the functionality you are entitled to with a subscription to 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.premium.cs  |
<table>
<thead>
<tr>
<th>Plugin ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
</table>
| com.snc.pa.premium.fm | Enables the functionality you are entitled to with a subscription to 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    |
| com.snc.pa.premium.hr | Enables the functionality you are entitled to with a subscription to 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 ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependecies</th>
</tr>
</thead>
</table>
| com.snc.pa.premium.itom | Enables the functionality you are entitled to with a subscription to 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 |
| com.snc.pa.premium.itos | Enables the functionality you are entitled to with a subscription to 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 | Inactive | false | com.snc.pa |
<table>
<thead>
<tr>
<th>Plugin ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
</table>
| com.snc.pa.premium.ppm | Enables the functionality you are entitled to with a subscription to 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 |
| com.snc.pa.premium.sir | Enables the functionality you are entitled to with a subscription to 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 ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependence</th>
</tr>
</thead>
</table>
| Performance Analytics Premium for Service Management | Enables the functionality you are entitled to with a subscription to 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 | Inactive | false | com.snc.pa |
| Performance Analytics Premium for Service Watch Insight | Enables the functionality you are entitled to with a subscription to 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 | Inactive | false | com.snc.pa |
<table>
<thead>
<tr>
<th>Plugin ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
</table>
| com.snc.pa.performance_analytics.premium.sam | Enables the functionality you are entitled to with a subscription to 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_analytics.premium.sam |
<p>| com.glide.performance_dashboards | Performance Dashboards | Active | false | com.glide.cms |
| com.snc.paas | Allows the development of custom applications to meet business needs. | Active | false | com.glideapp.workflow |
| com.snc.problem_management | Helps to identify the cause of a service interruption reported by a significant or recurring incidents. | Active | true | com.snc.service, com.glideapp.report.itsm |
| com.glideapp.report.itsm.prob.overview | Displays Problem Overview homepage. | Active | false | com.glideapp.report.itsm.prob.overview |
| com.snc.problem_task | Problem Task table with a reference to the Problem table. | Active | false | com.glideapp.report.itsm.prob.overview |
| com.snc.process_flow_formatter | Quickly summarizes multiple pieces of information about a process and displays the stages graphically at the top of a form. | Active | false | com.glideapp.report.itsm.prob.overview |
| com.snc.procurement | Allows users to create purchase orders and obtain items for fulfilling service catalog requests. | Inactive | true | com.glideapp.report.itsm.prob.overview |</p>
<table>
<thead>
<tr>
<th>Plugin ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Catalog</td>
<td>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.</td>
<td>Active</td>
<td>true</td>
<td>com.snc.product_catalog, com.glide.schedules, com.snc.planned_task_v2, com.snc.time_card, com.snc.skills_management, com.snc.process_flow_format, com.snc.cost_management, com.snc.project_management_db_views, com.snc.project_workbench, com.snc.timeline_visualization, com.glide.ui.checklist</td>
</tr>
<tr>
<td>Project Management_v3</td>
<td>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 Project Portfolio Suite with Financials plugin.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.project_management_v3</td>
</tr>
<tr>
<td>Project Management Teamspace 1</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>true</td>
<td>com.snc.financial_planning_pmo</td>
</tr>
<tr>
<td>Project Management Teamspace 2</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 3</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>Plugin 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>
</tr>
<tr>
<td>com.snc.ppm_management.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>com.snc.ppm_management.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>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 Project Portfolio Suite with Financials plugin.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.project_management, com.snc.demand_management, com.snc.resource_management, com.snc.sdlc.scrum.pp, com.snc.test_mgmt, com.snc.sdlc.scrum.ppm, com.snc.test_mgmt.ppm, com.snc.program_management</td>
</tr>
<tr>
<td>com.snc.financial_planning_pps</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</td>
</tr>
<tr>
<td>com.glide.protocol_profile.manager</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>Plugin 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>
</tr>
<tr>
<td>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>Defines push notification message queuing 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></td>
<td>Active</td>
<td>false</td>
<td>com.glide.push, com.glide.auxdb</td>
</tr>
<tr>
<td>Qualys Vulnerability Integration</td>
<td>Activates 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>com.snc.vulnerability</td>
</tr>
<tr>
<td>Query stats</td>
<td>Query stats.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.stats</td>
</tr>
<tr>
<td>Quiz Designer</td>
<td>Activates 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.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.assessment_designer.common, com.snc.assessment_core</td>
</tr>
<tr>
<td>Random Watermark Support</td>
<td>Generates unpredictable watermarks, and enable matching on these watermarks in inbound emails.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.mailbox</td>
</tr>
<tr>
<td>Rate Limit for REST API (New in London)</td>
<td>Provides rate limit support for REST API.</td>
<td>Active</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>Plugin 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>
</tr>
<tr>
<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>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>com.snc.release_management_v2</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>Inactive</td>
<td>true</td>
<td>com.snc.release_management, com.snc.planned_task, com.snc.process_flow_formatter</td>
</tr>
<tr>
<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>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>
<tr>
<td>com.glideapp.summary_report_engine</td>
<td>Causes 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>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, com.glideapp.report2</td>
</tr>
<tr>
<td>com.glideapp.report_stats</td>
<td>Provides reports and dashboards on reporting statistics.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glideapp.report</td>
</tr>
<tr>
<td>Plugin Name</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</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>
</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 Project Portfolio Suite with Financials plugin.</td>
<td>Inactive</td>
<td>true</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>
</tr>
<tr>
<td>REST API for global text search</td>
<td>com.glide.globalsearch</td>
<td>Provides a REST API for global text search.</td>
<td>Active</td>
<td>false</td>
</tr>
<tr>
<td>REST API Provider</td>
<td>com.glide.rest</td>
<td>Provides a REST API framework to support RESTful services.</td>
<td>Active</td>
<td>false</td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
</tr>
<tr>
<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>
</tr>
<tr>
<td>Role Delegation</td>
<td>com.snc.role_delegation</td>
<td>Delegation administrator to designate role delegators, who can delegate any role they have to members of their group.</td>
<td>Active</td>
<td>false</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>
</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>
</tr>
<tr>
<td>Scoped Analytics Framework</td>
<td>com.glide.scope.analytic.framework</td>
<td>Analytics Framework for Scoped Applications.</td>
<td>Active</td>
<td>false</td>
</tr>
<tr>
<td>Scoped Application Restricted Caller Access (New in London)</td>
<td>com.glide.scope.application.restricted.caller.access</td>
<td>Applications to restrict access to public tables and script includes.</td>
<td>Inactive</td>
<td>false</td>
</tr>
<tr>
<td>Script stats</td>
<td>com.glide.stats</td>
<td>Script stats.</td>
<td>Active</td>
<td>false</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>
</tr>
<tr>
<td>Script Whitelist Manager</td>
<td>com.glide.script.whitelist</td>
<td>Provides temporary support for continued direct invocation of whitelisted Java Packages, Constructors, and Methods.</td>
<td>Active</td>
<td>false</td>
</tr>
<tr>
<td>Scripted REST APIs</td>
<td>com.glide.scripted_rest_services</td>
<td>Provides framework for building Scripted REST APIs.</td>
<td>Active</td>
<td>false</td>
</tr>
<tr>
<td>Plugin 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>
</tr>
<tr>
<td>com.glide.scripted_rest_services.errors</td>
<td>An internal plugin component to Scripted REST APIs.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>com.glide.scripted_rest_services.internal</td>
<td>An internal plugin component to Scripted REST APIs</td>
<td>Active</td>
<td>false</td>
<td>com.glide.ui.css</td>
</tr>
<tr>
<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>com.glide.ui.scss</td>
<td>SCSS Content Provider.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<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>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>
<tr>
<td>com.snc.security_incident.analytics</td>
<td>Provides a unique 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.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.pa, com.snc.threat</td>
</tr>
<tr>
<td>com.snc.security_incident.response</td>
<td>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.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.service_management, com.snc.task_outage, com.snc.threat, com.snc.security_support, com.snc.wdp, com.snc.threat</td>
</tr>
<tr>
<td>Plugin ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependences</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Security Incident Response UI (Available in London Patch 2 only)</td>
<td>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.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.security_incident</td>
</tr>
<tr>
<td>Security Integration Framework (New in London)</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)</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>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
</tr>
<tr>
<td>--------</td>
<td>----</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
</tr>
<tr>
<td>Security Operations 'Have I Been Pwned' Integration</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>
</tr>
<tr>
<td>Security Operations ArcSight Logger Integration</td>
<td></td>
<td>Activates this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
</tr>
<tr>
<td>Security Operations Carbon Black Integration</td>
<td></td>
<td>Activates this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
</tr>
<tr>
<td>Security Operations CrowdStrike Host Integration</td>
<td></td>
<td>Activates this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
</tr>
<tr>
<td>Security Operations CrowdStrike Intelligence Integration</td>
<td></td>
<td>Activates this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
</tr>
<tr>
<td>Security Operations Elasticsearch Integration</td>
<td></td>
<td>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>
</tr>
<tr>
<td>Security Operations McAfee ESM Integration</td>
<td></td>
<td>Activates this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td>Inactive</td>
<td>false</td>
</tr>
<tr>
<td>Security Operations Exchange Microsoft Exchange Integration</td>
<td></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>
</tr>
<tr>
<td>Plugin 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>
</tr>
<tr>
<td>com.snc.secops.paloalto.autofocus</td>
<td>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.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.security_incident, com.snc.secops.orchestration</td>
</tr>
<tr>
<td>com.snc.secops.paloalto</td>
<td>Provides the ability to integrate the ServiceNow Security Incident Response application with the Palo Alto Networks Firewall application. 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, com.snc.secops.orchestration</td>
</tr>
<tr>
<td>com.snc.secops.paloalto.wildfire</td>
<td>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.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.security_incident, com.snc.secops.orchestration</td>
</tr>
<tr>
<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>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>Plugin Name</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Security Operations Spoke (New in London)</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>
</tr>
<tr>
<td>Security Operations Tanium Integration</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>
</tr>
<tr>
<td>Security Operations WHOIS Integration</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>
</tr>
<tr>
<td>Security Support Common</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>
</tr>
<tr>
<td>Security Support Orchestration</td>
<td>com.snc.security_support.orchestration</td>
<td>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.</td>
<td>Inactive</td>
<td>false</td>
</tr>
<tr>
<td>Self Service Password Reset</td>
<td>com.snc.password_reset</td>
<td>Provides locally authenticated users to request a temporary password if they forget their current password.</td>
<td>Active</td>
<td>false</td>
</tr>
<tr>
<td>Plugin ID</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
</tr>
<tr>
<td>-----------</td>
<td>----</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
</tr>
<tr>
<td>Self-Service Portal for Analytics</td>
<td>com.snc.pa.bi</td>
<td>Service Portal for Analytics - Allows users to request services related to dashboard access.</td>
<td>Inactive</td>
<td>false</td>
</tr>
<tr>
<td>Sentiment Analysis (New in London)</td>
<td>com.snc.sentiment_analysis</td>
<td>Sentiment Analysis used for Sentiment Analysis</td>
<td>Inactive</td>
<td>false</td>
</tr>
<tr>
<td>Server-side JavaScript Debugger</td>
<td>com.glide.debugger</td>
<td>Allows application developers and administrators to efficiently debug scripts that drive the applications they develop and support.</td>
<td>Active</td>
<td>false</td>
</tr>
<tr>
<td>Service Catalog CMS Extension</td>
<td>com.glideapp.servicecatalog.cms</td>
<td>Provides functionality to define the catalog experience within CMS.</td>
<td>Active</td>
<td>false</td>
</tr>
<tr>
<td>Service Catalog core applications</td>
<td>com.glideapp.servicecatalog</td>
<td>Allows users to order predefined, bundled goods and services from your IT organization or other departments.</td>
<td>Active</td>
<td>true</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>
</tr>
<tr>
<td>Service Catalog REST API</td>
<td>com.glideapp.servicecatalog.rest.api</td>
<td>Service Catalog REST API.</td>
<td>Active</td>
<td>false</td>
</tr>
<tr>
<td>Service Catalog Scoped API</td>
<td>com.glideapp.servicecatalog.scoped.api</td>
<td>Service Catalog Scoped API to support application API creation on Service Catalog platform.</td>
<td>Active</td>
<td>true</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>
</tr>
</tbody>
</table>

© 2019 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>Service Desk Call</td>
<td>com.snc.service_desk_call</td>
<td>Enables Service Desk staff to collect information in a call that does not relate to a specific process. The call is transferred to an incident, problem, change request or service catalog request.</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.glide.app.workflow, com.glide.schedules, com.glide.relative_duration</td>
</tr>
<tr>
<td>Service Level Management</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.glide.app.canvas, 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 Management Geolocation</td>
<td>com.snc.service_management_geolocation</td>
<td>Provides Service Management geolocation capabilities.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.geolocation</td>
</tr>
<tr>
<td>Plugin ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
<td>--------------</td>
<td></td>
</tr>
<tr>
<td>com.snc.service_management_geolocation_mobile</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, com.snc.service_management.geolocation.mobile</td>
<td></td>
</tr>
<tr>
<td>com.snc.service_modeling</td>
<td>Service Modeling used in Service Mapping and Delivery</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.vars, com.snc.command.enterprise</td>
<td></td>
</tr>
<tr>
<td>com.glide.service_portal.knowledge_base</td>
<td>Knowledge base for SP Base</td>
<td>Active</td>
<td>false</td>
<td></td>
<td></td>
</tr>
<tr>
<td>com.glide.service_portal.service_catalog</td>
<td>Enables Service Catalog widgets for Service Portal.</td>
<td>Active</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>com.glideapp.servicecatalog.portal</td>
<td>Enables Service Catalog widgets for Service Portal.</td>
<td>Active</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<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>
<td></td>
</tr>
<tr>
<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>
<td></td>
</tr>
<tr>
<td>com.glide.service_portal.config</td>
<td>Service Portal Configuration Pages.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.service-portal</td>
<td></td>
</tr>
<tr>
<td>com.glide.service_portal.designer</td>
<td>Drag-and-drop wysiwyg portal designer</td>
<td>Active</td>
<td>false</td>
<td>com.glide.service-portal</td>
<td></td>
</tr>
<tr>
<td>Plugin ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
<td>--------------</td>
<td></td>
</tr>
<tr>
<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, Services Status, and Social Q&amp;A.</td>
<td>Active</td>
<td>true</td>
<td>com.glide.service-portal, com.glide.service-portal.service-status, com.glide.service-portal.sqanda</td>
<td></td>
</tr>
<tr>
<td>com.glide.service-portal.sqanda</td>
<td>Service Portal Social QA.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.service-portal</td>
<td></td>
</tr>
<tr>
<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>
<td></td>
</tr>
<tr>
<td>com.snc.service_portfolio</td>
<td>A tool for 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.glideapp.servicecatalog, com.glideapp.summary_report_engine, com.glideapp.user_criteria</td>
<td></td>
</tr>
<tr>
<td>com.snc.service_portfolio.sla</td>
<td>A tool for commitments to be defined by an SLA, so that staff can track how efficiently the service desk meets commitments for a service offering.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.service_portfolio, com.snc.sla</td>
<td></td>
</tr>
<tr>
<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>
<td></td>
</tr>
<tr>
<td>com.glide.sessiondebug</td>
<td>Provides SessionDebug statements and filtering.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.app.sessiondebug</td>
<td></td>
</tr>
<tr>
<td>Plugin</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependence</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Signature Pad</td>
<td>com.snc.signaturepad</td>
<td>Provides a tool to allow a digital signature in a .pdf document.</td>
<td>Inactive</td>
<td>false</td>
<td>com.glide.db_images</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The Human Resources application uses this with various documents.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Activation of this plugin on production instances may require a separate license. Contact ServiceNow for details.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skills Management</td>
<td>com.snc.skills_management</td>
<td>Enables an administrator to assign configured competencies, called skills, to groups or individual users. These skills can then be used to determine which users and groups can be assigned particular tasks.</td>
<td>Inactive</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>Plugin ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependencies</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
<td>--------------</td>
<td></td>
</tr>
</tbody>
</table>
| **SLA Breakdowns**  
(New in London) | Provides the ability to generate breakdown data for each Task SLA record. For example, you can generate breakdown data on the basis of the Assignment group and Assigned to fields.  
**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. | **Active** | **false** | com.snc.sla.sla_breakdowns |
| **SLA Contract Add-on**  
| Extends the existing SLA functionality, by utilizing a contract as the master document that houses all appropriate data needed to drive the SLA processing of your task. | **Inactive** | **false** | com.snc.sla.contract2 |
| **SLA Timeline**  
| Provides the ability to view an SLA in a timeline. | **Active** | **false** | |
| **SM Planned Maintenance**  
<p>| 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. | <strong>Inactive</strong> | <strong>true</strong> | com.snc.service_management.core |</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>sn-custom-tinymce-scoped-app</td>
<td>com.sn-custom-tinymce-scoped-app</td>
<td>Scoped app providing custom tinymce build (New in London)</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>SNC Code Editor</td>
<td>com.glide.snc_code_editor</td>
<td>code_editor</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Social Q&amp;A</td>
<td>com.sn_kb_social_qa</td>
<td>Al lows users to ask and respond to questions and to vote on questions and answers. Social Q&amp;A extends the Knowledge application and uses existing Knowledge functionality such as user criteria and multiple knowledge bases.</td>
<td>Active</td>
<td>true</td>
<td>com.snc.knowledge3, com.glide.ui.ng.amb</td>
</tr>
<tr>
<td>Software Development Lifecycle (SDLC)</td>
<td>com.snc.sdlc</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.schn_dh</td>
<td>Special Handling Notes application demo data.</td>
<td>Inactive</td>
<td>false</td>
<td>com.sn_shn, com.snc.customerservice</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>
</tbody>
</table>

© 2019 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 ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Studio</td>
<td>Allows developers to add and update application files.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.code-search, com.sn_appcreator</td>
</tr>
<tr>
<td>Subscription Management and Enforcement Framework</td>
<td>Subscription Management and Enforcement Framework.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.usageanalytics, com.glide.subscription_framework</td>
</tr>
<tr>
<td>Subscription Based Notifications</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, com.glide.email_notification</td>
</tr>
<tr>
<td>Subscription Based Notifications 2.0</td>
<td>Subscription subscription model - improved and simplified.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.notification</td>
</tr>
<tr>
<td>Subscription and Activity Feed Framework</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>Survey Designer</td>
<td>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>Syntax Editor</td>
<td>Syntax Editor</td>
<td>Active</td>
<td>false</td>
<td>com.glide.snc_code_editor</td>
</tr>
<tr>
<td>System Applications Core</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>
</tr>
<tr>
<td>--------</td>
<td>----</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
</tr>
<tr>
<td>System</td>
<td>com.glide.system_import_sets</td>
<td>Provides the functionality for import sets.</td>
<td>Active</td>
<td>false</td>
</tr>
<tr>
<td>System</td>
<td>com.glide.system_update_sets (viewer)</td>
<td>Provides useful descriptions for update set entries and supports viewing contents of update sets.</td>
<td>Active</td>
<td>false</td>
</tr>
<tr>
<td>System</td>
<td>com.glide.system_update_sets_preview</td>
<td>All update set preview: viewing 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>
</tr>
<tr>
<td>System</td>
<td>com.glide.web_service_application</td>
<td>Provides a series of web service import sets.</td>
<td>Active</td>
<td>false</td>
</tr>
<tr>
<td>Tablet Device Support - iPad with iOS 6+</td>
<td>com.glide.ui.tablet</td>
<td>Provides a UI supporting nearly full-product functionality on the Apple iPad.</td>
<td>Inactive</td>
<td>false</td>
</tr>
<tr>
<td>Plugin 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>
</tr>
<tr>
<td>com.sn_publications</td>
<td>Provides a way to publish and send out newsletter like articles to targeted internal/external customers.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.cs_base</td>
</tr>
<tr>
<td>com.snc.publications Demo Data</td>
<td>Integrates Targeted Communications application demo data.</td>
<td>Inactive</td>
<td>true</td>
<td>com.sn_publications</td>
</tr>
<tr>
<td>com.snc.task_activities</td>
<td>Enables support for activities on task tables.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>com.snc.task_outage</td>
<td>Enables 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.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>com.snc.apps_hub</td>
<td>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.</td>
<td>Active</td>
<td>false</td>
<td>com.snc.apps, com.glide.ui.angular</td>
</tr>
<tr>
<td>com.sn_templated_snippet</td>
<td>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.</td>
<td>Inactive</td>
<td>true</td>
<td>com.glide.scope.access.restricted_caller</td>
</tr>
<tr>
<td>com.snc.test_mgmt</td>
<td>Provides a tool for manual software testing.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.planned_task_v2</td>
</tr>
<tr>
<td>com.snc.test_management.2.0 (New in London)</td>
<td>Enables you to manage testing processes and deliver software products more efficiently, with fewer errors.</td>
<td>Inactive</td>
<td>False</td>
<td>com.snc.planned_task_v2, com.snc.sdlc.agile.2.0.common</td>
</tr>
<tr>
<td>Plugin ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
<td>Dependency</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Text Index Attachments</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>Text Search - searching across multiple tables.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.text_index</td>
</tr>
<tr>
<td>Threat Core</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>Threat Intelligence - 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>Threat Intelligence Recorded Future - 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>Time card management</td>
<td>Time card management - 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>Plugin ID</td>
<td>Plugin Name</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
</tr>
<tr>
<td>com.snc.csm_time_recording</td>
<td>Time Recording for Customer Service (New in London)</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>
</tr>
<tr>
<td>com.snc.time_recording_fsm</td>
<td>Time Recording for Field Service (Changed in London)</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>
</tr>
<tr>
<td>com.snc.timeline_visualization</td>
<td>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>
</tr>
<tr>
<td>com.glide.tiny_url</td>
<td>Tiny URL Support</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>
</tr>
<tr>
<td>Plugin ID</td>
<td>ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
</tr>
<tr>
<td>-----------</td>
<td>----</td>
<td>-------------</td>
<td>-------</td>
<td>---------------</td>
</tr>
<tr>
<td>TinyMCE</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>
</tr>
<tr>
<td>Transaction Design Scope</td>
<td>com.glide.transaction_scope</td>
<td>Enables transaction design scope management.</td>
<td>Active</td>
<td>false</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>
</tr>
<tr>
<td>Transaction Stats</td>
<td>com.glide.stats</td>
<td>Transaction stats.</td>
<td>Active</td>
<td>false</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>
</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>
</tr>
<tr>
<td>Trusted Security Circles Client (Advanced)</td>
<td>com.snc.intel_sharing.client.adv</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>
</tr>
<tr>
<td>Plugin ID</td>
<td>Plugin ID</td>
<td>Description</td>
<td>State</td>
<td>Has Demo Data?</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------</td>
<td>-------------</td>
<td>-------</td>
<td>----------------</td>
</tr>
<tr>
<td>com.glide.ui.ui16</td>
<td>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>
</tr>
<tr>
<td>com.glide.system_update_set</td>
<td>Update Set Batching</td>
<td>Deploys update sets in a group.</td>
<td>Active</td>
<td>false</td>
</tr>
<tr>
<td>com.glide.upgrade_blame</td>
<td>Upgrade Blame Tool</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>
</tr>
<tr>
<td>com.glide.upgrade_metric</td>
<td>Upgrade Metric</td>
<td>Uses the Upgrade Metric table to track changes that take a long time to load during upgrades.</td>
<td>Active</td>
<td>false</td>
</tr>
<tr>
<td>com.glideapp.user_criteria.scoped.api</td>
<td>User Criteria Scoped API</td>
<td>User Criteria Scoped API to support CRUD operations on User Criteria.</td>
<td>Inactive</td>
<td>false</td>
</tr>
</tbody>
</table>

© 2019 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 ID</th>
<th>Description</th>
<th>State</th>
<th>Has Demo Data?</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<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>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>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>com.snc.vendor_ticket</td>
<td>Provides expanded functionality to obtain vendor performance data by tracking vendor incidents and SLAs.</td>
<td>Inactive</td>
<td>true</td>
<td>com.snc.service_portfolio, com.snc.service_portfolio, com.snc.task_outage, com.snc.vendor_performance</td>
</tr>
<tr>
<td>com.snc.version_management</td>
<td>Provides the ability to track, compare, and revert to multiple versions of table records.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>com.glideapp.version_support</td>
<td>Supports tracking versions of files that are stored in update sets, including the ability to compare and revert to previous versions.</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>
</tr>
<tr>
<td>--------</td>
<td>---------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
</tr>
<tr>
<td>VirusTotal Integration</td>
<td>com.snc.threat</td>
<td>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>
</tr>
<tr>
<td>Visual Task Board Flow Designer Spoke (New in London)</td>
<td>com.glide.ui.vtb.ah</td>
<td>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>
</tr>
<tr>
<td>Vulnerability Analytics</td>
<td>com.snc.vulnerability</td>
<td>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>Inactive</td>
<td>true</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>
</tr>
<tr>
<td>Plugin 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>
</tr>
<tr>
<td>Walk-up Experience (New in London)</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.glide.interaction, com.snc.asset_management, com.glide.service_portal</td>
</tr>
<tr>
<td>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>Web Service Import Set Tables</td>
<td>Complements web services and scripted web services in providing a web service interface to import set tables.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.web_service_import_set_tables, com.glide.web_service_application</td>
</tr>
<tr>
<td>Web Service Import Sets</td>
<td>Complements web services and scripted web services in providing a web service interface to import sets.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.vars, com.glide.system_property_categories, com.glide.system_import_set</td>
</tr>
<tr>
<td>Web Service Provider - Common</td>
<td>Provides the ability to create a scripted web service to accept any WSDL format.</td>
<td>Inactive</td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>Web Service Provider - Custom WSDL</td>
<td>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.</td>
<td>Active</td>
<td>false</td>
<td>com.glide.web_service_provider, com.glide.web_service_web_user_count, com.glide.web_service_web_user_count_web_service_provider</td>
</tr>
<tr>
<td>WebKit HTML to PDF</td>
<td>Enables the instance to use the service WebKit HTML to PDF.</td>
<td>Inactive</td>
<td>false</td>
<td>com.snc.platform.security.oauth</td>
</tr>
</tbody>
</table>
### ServiceNow plugins

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

#### How plugins are activated

Plugins may be added to the base platform in one of the following ways.

- Activated by default in the base ServiceNow system
- Activated by an admin user (not by default)
- Requested from ServiceNow before activating. This may be the case when a plugin is new, is appropriate for only certain deployments, and/or can only be activated by ServiceNow personnel.
- Plugins that are associated with a for-fee subscription to an application or suite can be activated only after your organization has purchased the subscription. See [View the applications and plugins that are included with a subscription](#).

---

<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.authoring</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.authoring</td>
</tr>
<tr>
<td>Workflow Pause Utility (New in London)</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.runtime</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.diagrammer, com.glide.vars, com.glide.schedules, com.glide.relative_duration, com.glide.web_service_application, com.glide.service_api, com.snc.datastructure, com.glideapp.live_feed</td>
</tr>
<tr>
<td>Workflow Stages element support (New in London)</td>
<td>com.glide.stage</td>
<td>Support for Workflow-type elements and stage displays.</td>
<td>Active</td>
<td>false</td>
<td></td>
</tr>
</tbody>
</table>

---

© 2019 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: After a plugin is active, you cannot disable or deactivate it. You can hide the functionality, if 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.

In some cases, a plugin cannot work at all unless one or more other plugins are 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 ask to continue, the system automatically activates all the plugins required.

In some 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 ask to continue, the system activates the requested plugin but does not include the features that depend on other plugins.

Request a plugin

Some plugins must be activated by ServiceNow personnel. These plugins do not appear in the System Definition > Plugins list.

Role required: none

Request the plugin through the HI Service Portal.

1. In the HI Service Portal, click Service Requests > Activate Plugin.
2. Fill out the form.

<table>
<thead>
<tr>
<th>Target Instance</th>
<th>Instance on which to activate the plugin.</th>
</tr>
</thead>
<tbody>
<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>Date and time must be at least 2 business days from the current time.</td>
</tr>
<tr>
<td>Reason/Comments</td>
<td>Provide any information that would be helpful for the ServiceNow personnel activating the plugin. For example, if you need the plugin activated at a specific time instead of during one of the default activation windows.</td>
</tr>
</tbody>
</table>

3. Click Submit.

Purchase a plugin

Some features require a separate subscription from the rest of the ServiceNow platform.

Role required: admin
To purchase a subscription, contact your ServiceNow account manager. In most cases, the account manager will arrange to have the plugin activated on your organization's production and non-production instances, generally within a few days. In some cases, you can activate the plugin within the instance.

If you do not have an account manager, decide to delay activation after purchase, or want to evaluate the feature on a non-production instance before purchase, follow the steps to activate a plugin. If the plugin is not listed in the System Definition > Plugins module, make a request through HI.

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 (🛠️), and add the **Package** column to the list.

3. Filter the list with these conditions to show only the components for the plugin:
   `(Package) (is) ( <plugin name>)`

4. In the **Class** column heading, click the menu icon (≡) and select **Group by Class**.

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

- **Category A**
  - Status: Completed
  - Progress: 100%
  - Edit

- **Category B**
  - Status: In progress
  - Progress: 33%
  - Continue

- **Category C**
  - Status: Not Started
  - Progress: 0%
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
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): Click to assign the tasks in this category to another user. The user must have access to the configuration tasks in the instance.
- **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.

### Available system properties

This page describes properties available to an instance.

Some properties are available on a system properties form, but some lesser-used properties are available only from the System Property (sys_properties) table. In some cases, the property does not exist in a base instance, but can be added if you need to change the value.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| com.glide.attachment.max_size | Sets the maximum file attachment size in megabytes. Leave the field empty to allow attachments up to a maximum of 1GB.  
- Type: integer  
- Default value: 1GB  
- 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 contain bad data, such as a row that is missing a column of data.  
- Type: true | false  
- Default value: false  
- Location: add 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 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 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 to the System Property (sys_properties) table |
| com.glide.soap.include_non_db_fields | Controls if non-database fields, such as the sys_tags field, are included in WSDLs and SOAP responses.  
- Type: true | false  
- Default value: false  
- Location: add to the System Property (sys_properties) table |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</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 to the System Property (sys_properties) table. |
  - Type: String  
  - Value: pa, html, script, include scripts, glide, custprefix, _sn  
  - Location: 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. Nonresponsive 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 if choice table selections marked as inactive (sys_choice inactive attribute = true) should be included when publishing an application.  
  - Type: integer  
  - 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 |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</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.hr.core.impersonateCheck | Allows a user to have identical permissions/access as the person they are impersonating.  

- Type: true | false  
- Default value: true  
- Location: System Property (sys_properties) table  

True - access and restrictions apply when impersonating another user.  
False - user has identical permissions/access as the person they are impersonating. |
| 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 a user's time zone  

- Type: true | false  
- Default value: false  
- Location: add to the System Property (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 |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</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.dd.publish_to_app_repo_enabled | Enables or disables display of the Publish To App Repo permission in Manage Developers.  
  - Type: integer  
  - Default value: true  
  - Location: System Property (sys_properties) table |
| com.snc.dd.publish_to_app_store_enabled | Enables or disables display of the Publish To App Store permission in Manage Developers.  
  - Type: integer  
  - Default value: true  
  - Location: System Property (sys_properties) table |
| com.snc.dd.publish_to_update_set_enabled | Enables or disables display of the Publish To Update Set permission in Manage Developers.  
  - Type: integer  
  - Default value: false  
  - Location: System Property (sys_properties) table |
| com.snc.dd.upgrade_app_enabled | Enables or disables display of the Update App permission in Manage Developers.  
  - Type: integer  
  - Default value: true  
  - 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 a script is allowed to run during a data collection cycle.  
  - Type: integer  
  - Default value: 30  
  - Location: System Property (sys_properties) table |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| com.snc.project.default_schedule          | Stores the sys_ID if 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_ganttt               | Automatically resubmits timed-out Ajax requests.  
  - Type: true | false  
  - Default value: false  
  - Location: Project > Administration > Properties                                                                                                                                                                                                                              |
| com.snc.task.associate_ci                | List of all the task types where user wants to associate CIs using a List system.  
  - Type: string  
  - Default: incident, change_request  
  - Location: System Property (sys_properties) table                                                                                                                                                                                                                             |
| com.snc.task.refresh_impacted_services   | List of all the task types where Refresh Impacted Services UI action is enabled.  
  - Type: string  
  - Default value: 50  
  - 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 of the task timer value based on changes to the task time worked records. This is accomplished through the Update task time business rule.  
  - Type: true | false  
  - Default value: false  
  - Location: System Property (sys_properties) table                                                                                                                                                                                                                             |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>css.assessment.caption.background.color</td>
<td>Sets the background color of the caption on assessment and survey questionnaires.</td>
</tr>
<tr>
<td></td>
<td>• Type: color</td>
</tr>
<tr>
<td></td>
<td>• Default value: #eee</td>
</tr>
<tr>
<td></td>
<td>• Location:</td>
</tr>
<tr>
<td></td>
<td>• Assessments &gt; Admin &gt; Assessment Properties</td>
</tr>
<tr>
<td></td>
<td>• Survey Management &gt; Administration &gt; Properties</td>
</tr>
<tr>
<td>css.assessment.caption.font.color</td>
<td>Sets the font color of the caption text on assessment and survey questionnaires.</td>
</tr>
<tr>
<td></td>
<td>• Type: color</td>
</tr>
<tr>
<td></td>
<td>• Default value: #ffffff</td>
</tr>
<tr>
<td></td>
<td>• Location:</td>
</tr>
<tr>
<td></td>
<td>• Assessments &gt; Admin &gt; Assessment Properties</td>
</tr>
<tr>
<td></td>
<td>• Survey Management &gt; Administration &gt; Properties</td>
</tr>
<tr>
<td>css.assessment.question.header.background.color</td>
<td>Sets the background color of question headers on assessment and survey questionnaires.</td>
</tr>
<tr>
<td></td>
<td>• Type: color</td>
</tr>
<tr>
<td></td>
<td>• Default value: #767676</td>
</tr>
<tr>
<td></td>
<td>• Location:</td>
</tr>
<tr>
<td></td>
<td>• Assessments &gt; Admin &gt; Assessment Properties</td>
</tr>
<tr>
<td></td>
<td>• Survey Management &gt; Administration &gt; Properties</td>
</tr>
<tr>
<td>css.$nav-highlight-main</td>
<td>Sets the color for the navigation expanded items highlight background</td>
</tr>
<tr>
<td></td>
<td>• Type: color</td>
</tr>
<tr>
<td></td>
<td>• Default Value: #3D4853</td>
</tr>
<tr>
<td></td>
<td>• Location: System Property (sys_properties) table</td>
</tr>
<tr>
<td>css.$nav-hr-color</td>
<td>Sets the color for the navigation separator</td>
</tr>
<tr>
<td></td>
<td>• Type: color</td>
</tr>
<tr>
<td></td>
<td>• Default Value: #303A46</td>
</tr>
<tr>
<td></td>
<td>• Location: System Property (sys_properties) table</td>
</tr>
<tr>
<td>css.$navpage-header-bg</td>
<td>Sets the color for the header background</td>
</tr>
<tr>
<td></td>
<td>• Type: color</td>
</tr>
<tr>
<td></td>
<td>• Default Value: #303A46</td>
</tr>
<tr>
<td></td>
<td>• Location: System Property (sys_properties) table</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>css.$navpage-header-color</td>
<td>Sets the color for the banner text</td>
</tr>
<tr>
<td></td>
<td>- Type: color</td>
</tr>
<tr>
<td></td>
<td>- Default Value: #FFFFFF</td>
</tr>
<tr>
<td></td>
<td>- Location: System Property (sys_properties)</td>
</tr>
<tr>
<td>css.$navpage-nav-bg-sub</td>
<td>Sets the color for the background for navigator and sidebars</td>
</tr>
<tr>
<td></td>
<td>- Type: color</td>
</tr>
<tr>
<td></td>
<td>- Default Value: #455464</td>
</tr>
<tr>
<td></td>
<td>- Location: System Property (sys_properties)</td>
</tr>
<tr>
<td>css.$navpage-nav-border</td>
<td>Sets the color for the border for UI16</td>
</tr>
<tr>
<td></td>
<td>- Type: color</td>
</tr>
<tr>
<td></td>
<td>- Default Value: #DDD</td>
</tr>
<tr>
<td></td>
<td>- Location: System Property (sys_properties)</td>
</tr>
<tr>
<td>css.$navpage-nav-color-sub</td>
<td>Sets the color for module text in UI16</td>
</tr>
<tr>
<td></td>
<td>- Type: color</td>
</tr>
<tr>
<td></td>
<td>- Default Value: #BEC1C6</td>
</tr>
<tr>
<td></td>
<td>- Location: System Property (sys_properties)</td>
</tr>
<tr>
<td>css.$navpage-nav-selected-bg</td>
<td>Sets the color for navigator selected tab background</td>
</tr>
<tr>
<td></td>
<td>- Type: color</td>
</tr>
<tr>
<td></td>
<td>- Default Value: #4B545F</td>
</tr>
<tr>
<td></td>
<td>- Location: System Property (sys_properties)</td>
</tr>
<tr>
<td>css.$navpage-nav-selected-color</td>
<td>Sets the color for the currently selected navigation tab icon color for UI16</td>
</tr>
<tr>
<td></td>
<td>- Type: color</td>
</tr>
<tr>
<td></td>
<td>- Default Value: #FFFFFF</td>
</tr>
<tr>
<td></td>
<td>- Location: System Property (sys_properties)</td>
</tr>
<tr>
<td>css.tablet.gradient.start</td>
<td>Start color of the gradient for the tablet UI header.</td>
</tr>
<tr>
<td></td>
<td>- Type: color</td>
</tr>
<tr>
<td></td>
<td>- Default value: #666</td>
</tr>
<tr>
<td></td>
<td>- Location: System Properties &gt; Tablet UI Properties</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| 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: lightgrey  
  - 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.apps.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 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 to the System Property (sys_properties) table |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.authenticate.sso.saml2.require_signed_authnrequest</td>
<td>Enables the Identity Provider’s Single sign on service to receive a signed AuthnRequest</td>
</tr>
<tr>
<td></td>
<td>• Type: true</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>glide.banner.image.url</td>
<td>URL used when clicking the banner image.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: home.do</td>
</tr>
<tr>
<td></td>
<td>• Location: System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.banner.image.url_target</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: gsft_main</td>
</tr>
<tr>
<td></td>
<td>• Location: System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.businessrule.async_condition_check</td>
<td>Specifies if the instance checks the condition statement of async business rules (the When field is set to async) prior to running the business rule. If this property is set to true, the instance evaluates the async business rule conditions a second time before running the rule. If this property is set to false or missing, the instance does not evaluate the conditions a second time.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: false</td>
</tr>
<tr>
<td></td>
<td>• Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.businessrule.callstack</td>
<td>Determines 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 need to know which business rules are running and in which order.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: false</td>
</tr>
<tr>
<td></td>
<td>• Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>glide.canvas.grid.widget_performance_threshold</strong></td>
<td>Defines the maximum number of seconds for a widget to render on a dashboard. Widgets that exceed this time are not rendered and a warning message displays. Users can click to restart rendering. Stopping widgets that render slowly enables faster widgets to load, and increases the speed of dashboard loading.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This system property applies to responsive dashboards only.</td>
</tr>
<tr>
<td></td>
<td>* Type: integer</td>
</tr>
<tr>
<td></td>
<td>* Default value: none</td>
</tr>
<tr>
<td></td>
<td>* Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td><strong>glide.canvas.grid.widget_render_concurrent_max</strong></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This system property applies to responsive dashboards only.</td>
</tr>
<tr>
<td></td>
<td>Two is the minimum value, and 1 is interpreted as 2. For values of zero or lower, all widgets load simultaneously.</td>
</tr>
<tr>
<td></td>
<td>* Type: integer</td>
</tr>
<tr>
<td></td>
<td>* Default value: none</td>
</tr>
<tr>
<td></td>
<td>* Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td><strong>glide.chart.decimal.precision</strong></td>
<td>Controls the rounding precision of non-currency numeric values displayed on reports. This property has a maximum possible value of 4. A <strong>Decimal Precision</strong> value specified in a report's style options overrides this property. Currency values always have a precision of 2.</td>
</tr>
<tr>
<td></td>
<td>* Type: integer</td>
</tr>
<tr>
<td></td>
<td>* Default value: 2</td>
</tr>
<tr>
<td></td>
<td>* Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>glide.chat.invite_fields</td>
<td>(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 users referenced by the fields to the chat room.</td>
</tr>
<tr>
<td></td>
<td>Type: string</td>
</tr>
<tr>
<td></td>
<td>Default value: none</td>
</tr>
<tr>
<td></td>
<td>Location: <strong>Social IT &gt; Chat Administration &gt; Properties</strong></td>
</tr>
<tr>
<td>glide.chat_room.create_roles</td>
<td>(Chat plugin) Comma-separated list of roles that are allowed to create chat rooms.</td>
</tr>
<tr>
<td></td>
<td>Type: string</td>
</tr>
<tr>
<td></td>
<td>Default value: none</td>
</tr>
<tr>
<td></td>
<td>Location: <strong>Social IT &gt; Chat Administration &gt; Properties</strong></td>
</tr>
<tr>
<td>glide.chat.show_emoticons</td>
<td>(Chat plugin) Enables or disables rendering text emoticons as images.</td>
</tr>
<tr>
<td></td>
<td>Type: true</td>
</tr>
<tr>
<td></td>
<td>Default value: true</td>
</tr>
<tr>
<td></td>
<td>Location: <strong>Social IT &gt; Chat Administration &gt; Properties</strong></td>
</tr>
<tr>
<td>glide.cmdb_model.display_name.shorten</td>
<td>When set to true, generates shorter display names for product models if the name of the product model contains the manufacturer name.</td>
</tr>
<tr>
<td></td>
<td>Type: true</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>glide.cookies.http_only</td>
<td>Enables (true) or disables (false) the generation of HTTP only cookies. Set this property to <strong>false</strong> to use Approval with E-Signature.</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>glide.cost_mgmt.calc_actual_cost</td>
<td>(Cost Management plugin) Sums all task expense lines and adds the total to the <strong>Work cost</strong> field on the task record when an expense line is created for any task with a <strong>Type</strong> of <strong>Planned task</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>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</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. This feature should only be enabled during initial testing or when troubleshooting because it can generate a large number of log records.  
  - Type: true | false  
  - Default value: false  
  - Location: System Property (sys_properties) table |
| glide.cost_mgmt.process_task_cis               | (Cost Management plugin) Creates expense lines to 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.  
  - 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.custom.ip.authenticate.allow             | comma-separated list or 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 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 - a comma-separated list of tables  
  - Location: System Property (sys_properties) table |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.db.clone.allow_clone_target</td>
<td>Enables (true) or disables (false) use of a non-production instance as the target for a system clone.</td>
</tr>
<tr>
<td></td>
<td>- Type: true</td>
</tr>
<tr>
<td></td>
<td>- Default value: false for production instances, true for non-production instances</td>
</tr>
<tr>
<td></td>
<td>- Location: System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.db.impex.XMLLoader.max.file.size.mb</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>- Type: integer</td>
</tr>
<tr>
<td></td>
<td>- Default value: 100</td>
</tr>
<tr>
<td></td>
<td>- Location: System Properties &gt; Import Export</td>
</tr>
<tr>
<td>glide.db.large.threshold</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>- Type: integer</td>
</tr>
<tr>
<td></td>
<td>- Default value: none</td>
</tr>
<tr>
<td></td>
<td>- Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.db.loguser</td>
<td>Display, or suppress display, of database errors (such as Unique Key violation detected by database (Duplicate entry 'ABC' for key 'name') to user.) to logged in user.</td>
</tr>
<tr>
<td></td>
<td>- Type: true</td>
</tr>
<tr>
<td></td>
<td>- Default value: none</td>
</tr>
<tr>
<td></td>
<td>- Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.db.max.aggregate.size</td>
<td>Sets the maximum number of groups a grouped report or list renders. Larger values may affect system performance.</td>
</tr>
<tr>
<td></td>
<td>- Type: integer</td>
</tr>
<tr>
<td></td>
<td>- Default value: 100</td>
</tr>
<tr>
<td></td>
<td>- Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>glide.db.max_view_records</td>
<td>Sets the maximum number of records returned when running a GlideRecord query in a script. Values larger than the default are not recommended as 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.</td>
</tr>
<tr>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 10000</td>
</tr>
<tr>
<td></td>
<td>• Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.db.table.update_inactive_choices_enabled</td>
<td>Specifies if choice table selections marked as inactive (sys_choice inactive attribute = true) should be loaded into client databases when applications are installed.</td>
</tr>
<tr>
<td></td>
<td>• Type: integer</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.discovery.application_mapping</td>
<td>Enables or disables the Application Dependency Mapping (ADM) feature.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</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>glide.discovery.log_message_chars</td>
<td>Specify the maximum length a log message can be before ServiceNow creates a preview for it in the list view. 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.</td>
</tr>
<tr>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 200 (Characters)</td>
</tr>
<tr>
<td></td>
<td>• Location: Discovery Definition &gt; Properties</td>
</tr>
<tr>
<td>glide.discovery.use_cmdb_identifiers</td>
<td>Controls whether Discovery uses the CMDB Identification and Reconciliation Framework, introduced with the Geneva release, or the legacy identifiers from previous releases.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: true</td>
</tr>
<tr>
<td></td>
<td>• Location: Discovery Definition &gt; Properties</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>glide.domain.notify_change</td>
<td>Displays a notification message telling the user that the domain picker automatically changed</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>glide.domain.notify_record_change</td>
<td>Displays a notification message telling the user that the domain picker automatically changed</td>
</tr>
<tr>
<td></td>
<td>because the record that the user is viewing changed the domain in which the user is in.</td>
</tr>
<tr>
<td></td>
<td>- Type: true</td>
</tr>
<tr>
<td></td>
<td>- Default value: false</td>
</tr>
<tr>
<td></td>
<td>- Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.ecmdb.all_relationship_role</td>
<td>An example value is: itil,asset,configuration.</td>
</tr>
<tr>
<td></td>
<td>- Type: string</td>
</tr>
<tr>
<td></td>
<td>- Default value: none</td>
</tr>
<tr>
<td></td>
<td>- Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.email.append.timezone</td>
<td>Specifies whether to append the time zone to all dates and times in outbound emails.</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 Properties &gt; Email</td>
</tr>
<tr>
<td>glide.email.forward_subject_prefix</td>
<td>Specifies the list of prefixes (comma-separated) in the subject line that identify a</td>
</tr>
<tr>
<td></td>
<td>forwarded email.</td>
</tr>
<tr>
<td></td>
<td>- Type: string</td>
</tr>
<tr>
<td></td>
<td>- Default value: fw:,fwd:</td>
</tr>
<tr>
<td></td>
<td>- Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.email.journal.lines</td>
<td>Specifies the number of entries from a journal field (such as Additional comments and Work</td>
</tr>
<tr>
<td></td>
<td>notes) included in email notifications. A value of -1 includes all journal entries.</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 &gt; Email</td>
</tr>
<tr>
<td>glide.email.mail_to</td>
<td>Specifies the email address to send notifications that use the ${mailto:} variable.</td>
</tr>
<tr>
<td></td>
<td>- Type: string</td>
</tr>
<tr>
<td></td>
<td>- Default value: SMTP email address that is active by default</td>
</tr>
<tr>
<td></td>
<td>- Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>glide.email.name_split</td>
<td>Delimiter between first and last name in an email address to identify users from incoming emails. For example, a delimiter of <code>'.'</code> (period) in the email address <a href="mailto:john.smith@company.com">john.smith@company.com</a> tells the system to look for a user record for John Smith.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: period (.)</td>
</tr>
<tr>
<td></td>
<td>• Location: System Properties &gt; Email</td>
</tr>
<tr>
<td>glide.email.notification.save_when_no_recipients</td>
<td>Controls whether 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.</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>glide.email.override.url</td>
<td>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: <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>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: Instance URL</td>
</tr>
<tr>
<td></td>
<td>• Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.email.read.active</td>
<td>Specifies whether to enable or disable the inbound mail server.</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 Properties &gt; Email</td>
</tr>
<tr>
<td>glide.email.reply_subject_prefix</td>
<td>Specifies the list of prefixes (comma-separated) in the subject line that identify an email reply.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: re:aw:,r:</td>
</tr>
<tr>
<td></td>
<td>• Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.email.smtp.active</td>
<td>Specifies whether to enable or disable the outgoing mail server.</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 Properties &gt; Email</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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 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 to the System Property (sys_properties) table |
| 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 to the 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:** Email clients that use the plain text version of the email still show the watermark.  
  - Type: true | false  
  - Default value: false  
  - Location: add to the System Property (sys_properties) table |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.email_client.show_sms_option</td>
<td>Specify whether a check box appears in the email client for sending the message to the user’s SMS device. If no SMS device exists, the email client sends the message to the primary email device.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: false</td>
</tr>
<tr>
<td></td>
<td>• Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.excel.max_cells</td>
<td>Sets the maximum number of cells in an Excel export.</td>
</tr>
<tr>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 500000</td>
</tr>
<tr>
<td></td>
<td>• Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.excel.use_user_date_format</td>
<td>Determines whether Excel exports use the date/time format specified in a user’s profile (true). If false, exports the instance date/time format defined by the glide.sys.date_format property.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: false</td>
</tr>
<tr>
<td></td>
<td>• Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.export.csv.charset</td>
<td>Specify the character set used to export CSV files. See Supported Character Encodings for a list of supported character encoding options.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: windows-1252</td>
</tr>
<tr>
<td></td>
<td>• Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.export.csv.raw.value</td>
<td>When true, raw database values are exported instead of the display values when you export to CSV. When false, display values are exported instead.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: false</td>
</tr>
<tr>
<td></td>
<td>• Location: System Properties &gt; Import Export</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>glide.export.escape_formulas</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>· Type: true</td>
</tr>
<tr>
<td></td>
<td>· Default value: true for new instances starting with Istanbul</td>
</tr>
<tr>
<td></td>
<td>· Location: System Property (sys_properties) table for new instances starting with Istanbul. For upgraded instances, add to the System Property table.</td>
</tr>
<tr>
<td>glide.export.excel.wrap_cells</td>
<td>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.</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 the property</td>
</tr>
<tr>
<td>glide.export.force_ui_list_behavior</td>
<td>When true, journal fields such as worknotes and comments are not included when you export records. When false, these fields are included.</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>glide.glidesoap.proxy_host</td>
<td>Specify the proxy server hostname or IP address for SOAP clients.</td>
</tr>
<tr>
<td></td>
<td>· Type: string</td>
</tr>
<tr>
<td></td>
<td>· Default value: value of glide.http.proxy_host</td>
</tr>
<tr>
<td></td>
<td>· Location: System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.glidesoap.proxy_port</td>
<td>Specify the port number for the proxy server for SOAP clients.</td>
</tr>
<tr>
<td></td>
<td>· Type: string</td>
</tr>
<tr>
<td></td>
<td>· Default value: value of glide.http.proxy_port</td>
</tr>
<tr>
<td></td>
<td>· Location: System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.help.default.page</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>· Type: string</td>
</tr>
<tr>
<td></td>
<td>· Default value: <a href="http://wiki.servicenow.com/">http://wiki.servicenow.com/</a></td>
</tr>
<tr>
<td></td>
<td>· Location: System Property (sys_properties) table</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>glide.history.max_entries</td>
<td>Sets the number of characters to display as a preview of journal input fields.</td>
</tr>
<tr>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 250</td>
</tr>
<tr>
<td></td>
<td>• Location: System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.home.page</td>
<td>Determines which page to load when a user selects a homepage from the banner.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: home_splash.do? sysparm_direct=true</td>
</tr>
<tr>
<td></td>
<td>• Location: System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.home.refresh_disabled</td>
<td>Determines whether homepage refresh is disabled (true) or enabled (false).</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: false</td>
</tr>
<tr>
<td></td>
<td>• Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.home.refresh_intervals</td>
<td>comma-separated list of refresh intervals available on homepages.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: 300,900,1800,3600</td>
</tr>
<tr>
<td></td>
<td>• Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.html.escape_script</td>
<td>Determines whether JavaScript tags are enabled (true) or disabled (false)</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.html.sanitize_all_fields</td>
<td>Determines whether all HTML fields are sanitized to remove unwanted code.</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.http.connection_timeout</td>
<td>Specify the maximum number of milliseconds an outbound HTTP request (such as Web Services) will wait to establish a connection.</td>
</tr>
<tr>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 10000 (10 seconds)</td>
</tr>
<tr>
<td></td>
<td>• Location: System Property (sys_properties) table</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| glide.http.proxy_bypass_list | Specify 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       | Specify the proxy server hostname or IP address  
  - Type: string  
  - Default value: none  
  - Location: System Property (sys_properties) table |
| glide.http.proxy_ntdomain   | Specify 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     | Specify 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 | Specify 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 | Specify the username used to authenticate the proxy server with NTLM authentication.  
  - Type: string  
  - Default value: none  
  - Location: System Property (sys_properties) table |
| glide.http.proxy_port       | Specify the port number for the proxy server  
  - Type: string  
  - Default value: none  
  - Location: System Property (sys_properties) table |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.http.proxy_password</td>
<td>Specify the password used to authenticate the proxy server.</td>
</tr>
<tr>
<td></td>
<td>- Type: string</td>
</tr>
<tr>
<td></td>
<td>- Default value: none</td>
</tr>
<tr>
<td></td>
<td>- Location: System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.http.proxy_username</td>
<td>Specify the username used to authenticate the proxy server.</td>
</tr>
<tr>
<td></td>
<td>- Type: string</td>
</tr>
<tr>
<td></td>
<td>- Default value: none</td>
</tr>
<tr>
<td></td>
<td>- Location: System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.http.timeout</td>
<td>(Web Service Consumer Plugin) Specifies the maximum number of milliseconds to wait before an outbound transaction times out.</td>
</tr>
<tr>
<td></td>
<td>- Type: integer</td>
</tr>
<tr>
<td></td>
<td>- Default value: 175000 (175 seconds)</td>
</tr>
<tr>
<td></td>
<td>- Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.i18n.force_index</td>
<td>Specifies that all translated fields are indexed regardless of the value of the table attribute text_index_translations.</td>
</tr>
<tr>
<td></td>
<td>- Type: true</td>
</tr>
<tr>
<td></td>
<td>- Default value: true</td>
</tr>
<tr>
<td>glide.image_provider.security_enabled</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>- Type: true</td>
</tr>
<tr>
<td></td>
<td>- Default value:</td>
</tr>
<tr>
<td></td>
<td>- New/zbooted instances: property is present and set to true</td>
</tr>
<tr>
<td></td>
<td>- Upgraded instances: false if property is not present, unchanged if property is present</td>
</tr>
<tr>
<td></td>
<td>- Location: Add the property to the System Property (sys_properties) table.</td>
</tr>
<tr>
<td>glide.imap.secure</td>
<td>Specifies whether to enable SSL encryption for connections to the IMAP server.</td>
</tr>
<tr>
<td></td>
<td>- Type: true</td>
</tr>
<tr>
<td></td>
<td>- Default value: false</td>
</tr>
<tr>
<td></td>
<td>- Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>glide.imap.secure_port</td>
<td>Specifies the communications port for IMAP secure connections.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: 995</td>
</tr>
<tr>
<td></td>
<td>• Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.imap.tls</td>
<td>Specifies whether to start the IMAP server in Transport Layer Security (TLS) mode.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: false</td>
</tr>
<tr>
<td></td>
<td>• Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.import.debug</td>
<td>Enables debug logging for all import processes.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: false</td>
</tr>
<tr>
<td></td>
<td>• Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.import.error_message.generic</td>
<td>When true, failed imports display a generic error instead of a verbose SQL message. Enabling this property is highly recommended.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: true for new instances starting with Istanbul, false for upgraded instances</td>
</tr>
<tr>
<td></td>
<td>• Location: System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.import.sftp.debug</td>
<td>Enables additional debug logging for SFTP imports.</td>
</tr>
<tr>
<td></td>
<td>Enables this property causes the instance to log all outgoing and incoming messages during the SSH session.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: false</td>
</tr>
<tr>
<td></td>
<td>• Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.import.scp.debug</td>
<td>Enables additional debug logging for SCP imports.</td>
</tr>
<tr>
<td></td>
<td>Enables this property causes the instance to log all outgoing and incoming messages during the SSH session.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: false</td>
</tr>
<tr>
<td></td>
<td>• Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>glide.import_set.preserve.leading.spaces</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The import process always removes trailing spaces from Excel data cells.</td>
</tr>
</tbody>
</table>
|                                                            | - Type: true | false  
|                                                            | - Default value: false  
|                                                            | - Location: add 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. 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: false  
|                                                            | - Location: add 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  
<p>|                                                            | - Location: add to the System Property (sys_properties) table  |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| glide.invalid_query.returns_no_rows      | Controls how invalid GlideRecord queries are handled. When this property is true, invalid queries always return no rows. When this property is false (default), if a query is incorrect, such as by including an invalid field name, 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)`.
<p>|                                           | To use this property, change the line <code>gr.addQuery('table', arguments.length == 1 ? record.getRecordClassName() : tableName);</code> in the Workflow script include to <code>gr.addQuery('table', (tableName) ? tableName : record.getRecordClassName() );</code>. |
|                                           | - Type: true | false  |
|                                           | - Default value: false |
|                                           | - Location: add to the System Property (sys_properties) table |
| glide.itil.assign.number.on.insert       | Controls whether a task number is generated and assigned on load (Create New) or on submit of the task. 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 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 to the System Property (sys_properties) table |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| glide.knowman.search.apply_role_based_security | When set to true, honors read access of knowledge bases or articles specified for roles. When set to 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: add to the 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 logged in user language.  
  - Type: string  
  - Default value: empty  
  - Location: System Property (sys_properties) table |
| glide.knowman.show_language_option | (Knowledge Management Internationalization Plugin v2) Determines whether the Language box appears (true) or is hidden (false) on articles with multiple translations.  
  - Type: true | false  
  - Default value: false  
  - Location: add 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 to the System Property (sys_properties) table |
| glide.knowman.show_links | Determines 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 |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| glide.ldap.allow_empty_group | Determines whether all members can be removed from an Active Directory security group.  
- Type: true | false  
- Default value: true  
- Location: add 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 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: add to the System Property (sys_properties) table. |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.live_feed.company_feed_exclude_groups</td>
<td>Controls whether messages posted to a public group appear (true) or are omitted (false) on the Company Feed.</td>
</tr>
</tbody>
</table>
|                                                |   · 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 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 a large number of 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 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 to the 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  
<p>|                                                |   · Location: add to the System Property (sys_properties) table                                                                                                                                       |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</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 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 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.  
- 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.                                                                 |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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.user_notification_disabled | Logs recipients who are excluded because the **Notification** field is set to **Disabled** 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.include_logging                        | Enables or disables logging all reasons a recipient was included. This property is a master switch. If it is set to true, the subsequent properties dealing with the inclusion of logging are enabled. If it is set to false, none of the subsequent properties relating to the inclusion of logging are enabled.  
- 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.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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| glide.notification.recipient.include_logging.event_parm1 | Logs recipients who are included because they are in the parm1 or parm2 fields of the event record.  
• 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.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.  
• 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.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.  
• 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.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.  
• 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. |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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.                                                                                           · 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.recipient_users          | Logs recipients who are included via notification record’s Users field (recipient_users).                                                                                                                                             · 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.subscription             | Logs recipients because they are subscribed via User Notification Preferences.                                                                                                                                                                      · 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.pdf_export_from_form_list.show_report_attrs                    | Enables or disable displaying the PDF page header for all PDFs generated from a list.                                                                                                                                             · Type: true | false  
· Default value: true  
· Location: add to the 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 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 to the System Property (sys_properties) table |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.pg.any_rejection_rejects</td>
<td>Controls the default process guide rejection handling. If this property is set to true, the first rejection rejects the entity. If false, all users must reject the approval.</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.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 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.</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>glide.phone_number_e164.display_national</td>
<td>Determines how a Phone Number (E164) field displays phone numbers. 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.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: false</td>
</tr>
<tr>
<td></td>
<td>• Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.phone_number_e164.display_territory_selector</td>
<td>Determines whether to display the territory selector. Hiding the territory selector restricts users to entering only local or national phone numbers.</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>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>glide.phone_number_e164.display_territory_text</td>
<td>Determines when a Phone Number (E164) field displays a territory label. 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.</td>
</tr>
</tbody>
</table>
|                                           |   - Type: string  
|                                           |   - Default value: read-only  
|                                           |   - Location: add to the System Property (sys_properties) table  |
| glide.phone_number_e164.display_users_idd  | Determines whether to display the international direct dialing prefix between the territory selector and the input box on forms.                                                                                   |
|                                           |   - Type: true|false  
|                                           |   - Default value: false  
|                                           |   - Location: add to the System Property (sys_properties) table  |
| glide.phone_number_e164.strict            | Determines 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  
<p>|                                           |   - Location: add to the System Property (sys_properties) table  |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.pop3.ignore_headers</td>
<td>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 (<em>) for the subtype. For example, &quot;Content-Type:multipart/</em>; report-type=delivery-status:&quot; ignores emails containing a type of multipart and a parameter of report-type=delivery-status. For syntax specifications, see <a href="http://www.w3.org/Protocols/rfc1341/4_Content-Type.html">http://www.w3.org/Protocols/rfc1341/4_Content-Type.html</a>.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: Auto-Submitted:auto-replied,X-FC-MachineGenerated:true,Content-Type:multipart/report; report-type=delivery-status;</td>
</tr>
<tr>
<td></td>
<td>• Location: <strong>System Properties</strong> &gt; <strong>Email</strong></td>
</tr>
<tr>
<td>glide.pop3.ignore_senders</td>
<td>Specifies the comma-separated list of senders that cause the instance to ignore an email message. Enter only the name before the at (@) sign.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: mailer-daemon, postmaster</td>
</tr>
<tr>
<td></td>
<td>• Location: <strong>System Properties</strong> &gt; <strong>Email</strong></td>
</tr>
<tr>
<td>glide.pop3.ignore_subjects</td>
<td>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. These values are case-insensitive.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: out of office autoreply, undeliverable:, delivery failure:, returned mail:, autoreply</td>
</tr>
<tr>
<td></td>
<td>• Location: <strong>System Properties</strong> &gt; <strong>Email</strong></td>
</tr>
<tr>
<td>glide.pop3.parse_end</td>
<td>(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.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: none</td>
</tr>
<tr>
<td></td>
<td>• Location: <strong>System Properties</strong> &gt; <strong>Email</strong></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>glide.pop3.parse_start</td>
<td>(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.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: none</td>
</tr>
<tr>
<td></td>
<td>• Location: System Properties &gt; Email</td>
</tr>
<tr>
<td>glide.pop3.process_locked_out</td>
<td>Enables (true) or disables (false) the ability for locked out users to trigger inbound actions.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: false</td>
</tr>
<tr>
<td></td>
<td>• Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.pop3.reply_separators</td>
<td>Specifies the 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.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: \n\n-----Original Message-----, \n\n______ \n\nFrom:</td>
</tr>
<tr>
<td></td>
<td>• Location: System Properties &gt; Email</td>
</tr>
<tr>
<td>glide.pop3readerjob.create_caller</td>
<td>Controls the behavior when an instance receives an email from an email address not associated with a user record. If this property is set to true, ServiceNow creates a new user record for the email address and places that new user in the Caller field of any created tickets. If the property is set to false, ServiceNow associates the new ticket to the Guest user record.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: false</td>
</tr>
<tr>
<td></td>
<td>• Location: System Properties &gt; Email</td>
</tr>
<tr>
<td>glide.processor.json.row_limit</td>
<td>Specify the maximum number of rows a JSON query returns</td>
</tr>
<tr>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 250</td>
</tr>
<tr>
<td></td>
<td>• Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.product.description</td>
<td>The value of this property is displayed as text in the banner next to the company logo</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: Service Management</td>
</tr>
<tr>
<td></td>
<td>• Location: System Properties &gt; Basic Configuration UI16</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| glide.product.help_url | Controls whether the help icon, help.gif, 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.help_show | The Banner image displayed for UI16 Interface  
- Type: uploaded image  
- Default value: None  
- Location: System Properties > Basic Configuration UI16 |
| glide.product.image.light | 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 "ServiceNow" in the browser's 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 it, 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 what quotas are matched to transactions.  
- Type: true | false  
- Default value: true  
- Location: add to the System Property (sys_properties) table |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.quota.manager.heartbeat</td>
<td>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 it writes status in the log file.</td>
</tr>
<tr>
<td></td>
<td>- Type: integer</td>
</tr>
<tr>
<td></td>
<td>- Default value: 1</td>
</tr>
<tr>
<td></td>
<td>- Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.quota.manager.minimum_transaction_time</td>
<td>Sets 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 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.</td>
</tr>
<tr>
<td></td>
<td>- Type: integer</td>
</tr>
<tr>
<td></td>
<td>- Default value: 1</td>
</tr>
<tr>
<td></td>
<td>- Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.remote_glide_record.max_count</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>- Type: integer</td>
</tr>
<tr>
<td></td>
<td>- Default value: 250</td>
</tr>
<tr>
<td></td>
<td>- Location: add to the System Property (sys_properties) table</td>
</tr>
</tbody>
</table>

**Caution:** 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.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.report.calendar.max_more_events_per_day</td>
<td>Defines that maximum number of calendar events that can appear in the +&lt;number&gt; popup for:</td>
</tr>
<tr>
<td></td>
<td>· A calendar day when calendar is in month or year view</td>
</tr>
<tr>
<td></td>
<td>· The top ‘full day’ section of a calendar day when a calendar is in day or week view</td>
</tr>
<tr>
<td></td>
<td>When this number is exceeded, a + many link appears, which opens a list of events instead of a popup. 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.</td>
</tr>
<tr>
<td></td>
<td>· Type: integer</td>
</tr>
<tr>
<td></td>
<td>· Default value: 30</td>
</tr>
<tr>
<td></td>
<td>· Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.report.calendar.max_events_displayed_per_cell</td>
<td>Defines the maximum number of events that can appear in calendar report for:</td>
</tr>
<tr>
<td></td>
<td>· A calendar day when calendar is in month or year view</td>
</tr>
<tr>
<td></td>
<td>· The top ‘full day’ section of a calendar day when a calendar is in day or week view</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>· Type: integer</td>
</tr>
<tr>
<td></td>
<td>· Default value: 3</td>
</tr>
<tr>
<td></td>
<td>· Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.report.new_calendar</td>
<td>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.</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>glide.report_home.group_report.show_usr_grp</td>
<td>Enables (true) or disables (false) the Reporting preferences link in the user's profile.</td>
</tr>
<tr>
<td></td>
<td>· Type: true</td>
</tr>
<tr>
<td></td>
<td>· Default value: false</td>
</tr>
<tr>
<td></td>
<td>· Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
</tbody>
</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: add to the 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 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 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 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 to the System Property (sys_properties) table |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.sc.reset_cascade</td>
<td>If true, forces variable cascading when navigating between pages in an order guide.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: false</td>
</tr>
<tr>
<td></td>
<td>• Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.schedules.repeat_nth</td>
<td>Controls how a schedule entry with <strong>Repeats</strong> set to <strong>Monthly</strong> and <strong>Monthly Type</strong> set to <strong>Day of the Week</strong> is defined. Choices are <strong>Week</strong> or <strong>Day</strong>. The <strong>Week</strong> option is defined as choosing a day of the month in the nth week selects the nth day of the month. The <strong>Day</strong> option is defined as choosing the nth day of the month selects the nth day of the month.</td>
</tr>
<tr>
<td></td>
<td>• Type: choice list</td>
</tr>
<tr>
<td></td>
<td>• Default value: day</td>
</tr>
<tr>
<td></td>
<td>• Location: sys_properties table</td>
</tr>
<tr>
<td>glide.schedules.fifth</td>
<td>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 <strong>Last</strong>, <strong>Next</strong>, and <strong>Strict</strong>. The <strong>Last</strong> option selects the last (fourth) day of the month. The <strong>Next</strong> option selects the first day of the next month. The <strong>Strict</strong> option skips the day completely. This property is only valid when the glide.schedules.repeat_nth property is set to <strong>Day</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Type: choice list</td>
</tr>
<tr>
<td></td>
<td>• Default value: last</td>
</tr>
<tr>
<td></td>
<td>• Location: sys_properties table</td>
</tr>
<tr>
<td>glide.script.ccsi.ispublic</td>
<td>Provides privacy control over client-callable script includes that are accessed by public pages. When this property is set to <strong>false</strong>, all client-callable script includes are private.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: false</td>
</tr>
<tr>
<td></td>
<td>• Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.script.log_level</td>
<td>Controls the behavior of gs.log. Set this property to <strong>none</strong> to disable Glide script logging, or <strong>print</strong> to save log data to the filesystem instead of the database. Use the default value <strong>all</strong> to save all Glide script logs to the database.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: all</td>
</tr>
<tr>
<td></td>
<td>• Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>glide.script_processor.admin</td>
<td>Specifies the user role necessary to access the Scripts - Background module. To require administrators to elevate privileges to access this module, set the value to security_admin.</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>glide.secondary.query.sysid</td>
<td>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 set to 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.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</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>glide.security.auto.resubmit.ajax</td>
<td>Automatically resubmits timed-out Ajax requests.</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>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>glide.security.checkacl.before.setvalue</td>
<td>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 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.</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>glide.security.csrf.handle.ajax.timeout</td>
<td>Handles errors for timed out Ajax requests.</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>glide.security.csrf.strict.validation.mode</td>
<td>Enforces strict validation on CSRF tokens so that users cannot resubmit a request if the CSRF token does not match.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</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>glide.security.diag_txns_acl</td>
<td>Controls who can view the stats.do, threads.do, and replication.do pages. When set to true, only administrators or users from a known IP address are allowed to view the pages. When set to false, all users have access to the pages.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: false</td>
</tr>
<tr>
<td></td>
<td>• Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| glide.security.disable_ui_pages_sysparm_client_script | Client scripts that are passed in URL parameter in UI pages are not evaluated by the system. If you use URL parameters to load client scripts, you can add and disable this system property. Only use this property 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 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 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: add to the System Property (sys_properties) table |
| glide.security.strict_elevate_privilege | Forces all elevated roles to be treated equally for users with the administrator role. When enabled, administrators need to explicitly, manually elevate themselves to any roles that are marked as elevated.  
  
  When disabled, administrators only need 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, administrators must add this property to the System Property (sys_properties) table |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 or not 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 |
| 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 to the System Property (sys_properties) table |
| glide.smtp.dateformat | Specify the date format to use for outgoing email notifications  
  - Type: string  
  - Default value: date format listed in email sender's user record (sys_user.date_format)  
  - Location: add 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 only recognizes 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 |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.smtp.fail_message_ids</td>
<td>Specifies the comma-separated list of SMTP error codes that prevent the instance from resending email.</td>
</tr>
<tr>
<td></td>
<td>· Type: string</td>
</tr>
<tr>
<td></td>
<td>· Default value: 500,501,502,503,504,550,551,552,553,554</td>
</tr>
<tr>
<td></td>
<td>· Location: <strong>System Properties &gt; Email</strong></td>
</tr>
<tr>
<td>glide.smtp.timeformat</td>
<td>Specify the time format to use for outgoing email notifications</td>
</tr>
<tr>
<td></td>
<td>· Type: string</td>
</tr>
<tr>
<td></td>
<td>· Default value: time format listed in email sender's user record (sys_user.time_format).</td>
</tr>
<tr>
<td></td>
<td>· Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.soap.allow_null_numeric_output</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The property <strong>glide.wsdl.show_nillable</strong> must be true to allow null values in SOAP responses.</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>glide.soap.default_security_policy</td>
<td>Specifies the name of SOAP security policy the instance uses when enforcing Web Services-Security (WSS) for inbound requests.</td>
</tr>
<tr>
<td></td>
<td>· Type: string</td>
</tr>
<tr>
<td></td>
<td>· Default value: default security policy</td>
</tr>
<tr>
<td></td>
<td>· Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>glide.soap.import_set_insert_serialized.&lt;tablename&gt;</td>
<td>Controls the processing of web service inserts. When this property is set to true, the instance processes multiple simultaneous inserts one at a time (serially across nodes) to ensure an accurate transform. Serialized processing slows down the speed at which the instance processes inserts. When this property is set to 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.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip:</strong> Only set this value to false to optimize for performance when the related transform map does not have a coalesce value that may be present simultaneously.</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>glide.soap.request_processing_timeout</td>
<td>Sets the maximum number of seconds 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.</td>
</tr>
<tr>
<td></td>
<td>- Type: integer</td>
</tr>
<tr>
<td></td>
<td>- Default value: 175 (value of glide.http.timeout divided by 1000)</td>
</tr>
<tr>
<td></td>
<td>- Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.spell.dictionary.en</td>
<td>Sets the spell checker dictionary used in the system for English users. There are dictionaries available for Brazilian Portuguese, Dutch, English US, English UK, French, German, Italian, Portuguese, Russian, Spanish, and Thai.</td>
</tr>
<tr>
<td></td>
<td>- Type: choice list</td>
</tr>
<tr>
<td></td>
<td>- Default value: en.dic (English US)</td>
</tr>
<tr>
<td></td>
<td>- Location: System Property (sys_properties) table</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>glide.spell.dictionary.max_matches</td>
<td>Sets the maximum number of spelling errors the spell-check should detect. By default it finds only 10 spelling errors. The instance ignores any additional errors after reaching the maximum value.</td>
</tr>
<tr>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 10</td>
</tr>
<tr>
<td></td>
<td>• Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.sys.activity_using_audit_direct</td>
<td>(Not Supported) Controls whether the record's history is generated using the Audit table (true) or not (false).</td>
</tr>
<tr>
<td></td>
<td>(Required) Set the value to false to generate history with History Sets.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</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>glide.sys.audit_inserts</td>
<td>Controls whether the Audit table audits inserts (true) or not (false).</td>
</tr>
<tr>
<td></td>
<td>• Type: true</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>glide.sys.date_format</td>
<td>System date format for all users unless overridden in the user's record</td>
</tr>
<tr>
<td></td>
<td>• Type: date format</td>
</tr>
<tr>
<td></td>
<td>• Default value: yyyy-MM-dd</td>
</tr>
<tr>
<td></td>
<td>• Location: System Properties &gt; Basic Configuration UI16</td>
</tr>
<tr>
<td>glide.sys.default.tz</td>
<td>System timezone for all users unless overridden in the user's record</td>
</tr>
<tr>
<td></td>
<td>• Type: timezone</td>
</tr>
<tr>
<td></td>
<td>• Default Value: none</td>
</tr>
<tr>
<td></td>
<td>• Location: System Properties &gt; Basic Configuration UI16</td>
</tr>
<tr>
<td>glide.sys.time_format</td>
<td>System time format for all users unless overridden in the user's record</td>
</tr>
<tr>
<td></td>
<td>• Type: time format</td>
</tr>
<tr>
<td></td>
<td>• Default Value: HH:mm:ss</td>
</tr>
<tr>
<td></td>
<td>• Location: System Properties &gt; Basic Configuration UI16</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| glide.sys_reference_row_check             | Controls whether the script conditions of Access Control Rules apply to a table’s reference fields.  
- Type: true | false  
- Default value: false  
- Location: add 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.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 to the System Property (sys_properties) table                                                                                                                                                                                                                                                                                                                                                |
| 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.  
- Type: true | false  
- Default value: false  
- Location: add to the System Property (sys_properties) table                                                                                                                                                                                                                                                                                                                                                   |
| glide.ts.index.attachment.list_terms.debug| When the value is set to **true**, the system 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.  
- Type: true | false  
- Default value: false  
- Location: add to the System Property (sys_properties) table                                                                                                                                                                                                                                                                                                                                          |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.ts.reindex.sys_metadata.after.upgrade</td>
<td>When the value is set to <strong>true</strong>, the system automatically reindexes the sys_metadata table after an upgrade, without noticeable performance impact. To disable this automatic reindexing, set this value to <strong>false</strong>.</td>
</tr>
</tbody>
</table>
|                                                        | - Type: true | false  
|                                                        | - Default value: true  
|                                                        | - Location: add to the System Property (sys_properties) table  |
| glide.ui.activity.displayname                          | Determines whether the activity formatter shows **name** values (true) or **user_name** values (false).                                                                                                    |
|                                                        | - Type: true | false  
|                                                        | - Default value: false  
|                                                        | - Location: add 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 to the System Property (sys_properties) table  |
| glide.ui.activity.email.use_display                    | Specifies whether to display email addresses or the user IDs (display value of the User table) in email headers. If true, the instance searches for a user record with a matching email address. If it cannot find a matching user record, it displays the email address. |
|                                                        | - Type: true | false  
|                                                        | - Default value: false  
|                                                        | - Location: add 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 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  
<p>|                                                        | - Location: add to the System Property (sys_properties) table  |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</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: This property 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 525px width and 350px 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 525px width and 350px height. If 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: WhiteSmoke  
- Location: System Property (sys_properties) table |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Default value</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.ui.activity.style.work_notes</td>
<td>Changes the background color of the activity stream work notes in UI15.</td>
<td>string</td>
<td>background-color: LightGoldenRodYellow</td>
<td>System Property (sys_properties) table</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>glide.ui.allow_deep_html_validation</td>
<td>Allows administrators to prevent users from saving invalid HTML in a journal field.</td>
<td>true</td>
<td>false</td>
<td>add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>glide.ui.attachment.force_download_all_mime_types</td>
<td>Forces download of all attachment files.</td>
<td>true</td>
<td>false</td>
<td>add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>glide.ui.audit_deleted_tables</td>
<td>comma-separated list of system tables for which the audit history tracks deletions.</td>
<td>string</td>
<td>sys_user, sys_user_group, sys_user_role, sys_user_has_role, sys_user_grmember, sys_group_has_role, sys_security_acl_role</td>
<td>System Property (sys_properties) table</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>glide.ui.auto.recovery</td>
<td>Allows users to recover unsaved changes while working in the developer studio.</td>
<td>true</td>
<td>false</td>
<td>Auto Recovery &gt; Properties</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>glide.ui.auto.recovery.exclude.field.types</td>
<td>comma-separated list of field types you want to exclude from automatic recovery.</td>
<td>string</td>
<td>none</td>
<td>Auto Recovery &gt; Properties</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>glide.ui.auto.recovery.unsupported.field.types</td>
<td>comma-separated list of field types excluded from automatic recovery.</td>
<td>string</td>
<td>password, password2, glide_encrypted, video, user_image, image</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| glide.ui.auto.recovery.unsupported.tables                           | comma-separated list of tables you want to exclude from automatic recovery.                                                                                     | Type: string  
  Default value: v_ws_editor  
  Location: Auto Recovery > Properties |
| glide.ui.auto_req.extend.session                                    | When set to true, this property enables the user to extend their user session by selecting a homepage refresh time. When set to 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's page refreshes every x number of minutes. The user's 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 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 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 to the System Property (sys_properties) table |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| glide.ui.chart.height                   | Specifies the height of a chart in pixels.  
- Type: integer  
- Default value: 300  
- Location: add 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 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 in order to display their labels.  
- Type: integer  
- Default value: 8  
- Location: add to the System Property (sys_properties) table |
| glide.ui.clickthrough.popup             | For reference fields, enables (true) or disables (false) displaying the pop-up diamond icon for reference fields and opening a new window when the icon is clicked.  
For document ID fields, enables (true) or disables (false) displaying the information icon and opening a pop-up window with the document's form. For more information, see 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 clickthrough icons for reference fields.  
- Type: true | false  
- Default value: false  
- Location: System Property (sys_properties) table |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| glide.ui.date_format.first_day_of_week   | Specifies which day of the week that weeks start on for calendar reports. Values: 1=Sunday, 2=Monday  
  - Type: integer  
  - Default value: 1  
  - Location: add to the 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: add to the 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 that user opens if no applications are opened via user preferences.  
  - Type: string  
  - Default value: first authorized application for the user  
  - Location: add 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.  
  - Note: This property is true by default.  
  - Type: true | false  
  - Default value: true  
  - Location: add to the System Property (sys_properties) table                                                                                                                                                                                                                      |
| glide.ui.doctype                          | Enables or disables the UI15 interface.  
  - Type: true | false  
  - Default value: true  
  - Location: System Property (sys_properties) table                                                                                                                                                                                                                                   |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| glide.ui.email_client.autocomplete.count                   | Sets the maximum number of auto-complete matches the Email Client displays. Type: integer
|                                                            | · Default value: 10                                                                                                                             |
|                                                            | · Location: **System Properties > Email**                                                                                                       |
| glide.ui.email_client.autocomplete.group                   | Specifies whether groups are included in auto-complete results for the Email Client. Type: true | false                                                                                       |
|                                                            | · Default value: true                                                                                                                           |
|                                                            | · Location: **System Properties > Email**                                                                                                       |
| glide.ui.email_client.email_address.disambiguator         | Sets the columns from the User (sys_user) table that the auto-complete list displays. Separate each column name with a semicolon character (;). See the system dictionary for a list of available column names. For example, add the sys_user.email and sys_user.company columns to show a user's email address and company in the auto-complete list. Type: string
<p>|                                                            | · Default value: first_name;last_name                                                                                                          |
|                                                            | · Location: add to the System Property (sys_properties) table                                                                               |
| glide.ui.email_client.from                                 | Specifies whether to display the <strong>From:</strong> line in the Email Client. Users can change the email address in the <strong>From:</strong> line by entering a new value. Type: true | false                                                                                       |
|                                                            | · Default value: false                                                                                                                         |
|                                                            | · Location: <strong>System Properties &gt; UI Properties</strong>                                                                                               |
| glide.ui.email_client.reply_to                             | Specifies whether to display the <strong>Reply to:</strong> line in the Email Client. Type: true | false                                                                                       |
|                                                            | · Default value: false                                                                                                                         |
|                                                            | · Location: <strong>System Properties &gt; UI Properties</strong>                                                                                               |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</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 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 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 they want to be the default for homepage gauges.  
- Type: string  
- Default value: portal  
- Location: System Property (sys_properties) table |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</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 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 | Determines which HTML field editor to use, TinyMCE or htmlArea (legacy).  
  - Type: string  
  - Default value: tinymce  
  - Location: **System Properties > UI Properties** |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| glide.ui.html.editor.extended_valid_elements | Defines which elements remain in the Tiny MCE text when the editor saves. This functionality can be very 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 the TinyMCE editor 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 the TinyMCE editor is enabled. The spellchecker tool is not supported in UI16 or UI15.  
  - Type: string  
  - Location: System Properties > UI Properties |
| 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.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 personalized, this property updates 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 to the System Property (sys_properties) table |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.ui.incident_alert_activity.fields</td>
<td>Incident communication plan activity formatter fields. This is the list of fields tracked from the Incident Communication Plan form in the activity formatter.</td>
</tr>
<tr>
<td></td>
<td>- Type: string</td>
</tr>
<tr>
<td></td>
<td>- Default value: opened_by, work_notes, comments, severity, estd_distruption_time, actual_disruption_time</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>glide.ui.js_error_notify</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>- Type: true</td>
</tr>
<tr>
<td></td>
<td>- Default value: true</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>glide.ui.label.enable</td>
<td>Enables (true) or disables (false) using labels, such as Most Active, Most Recent, or user created.</td>
</tr>
<tr>
<td></td>
<td>- Type: true</td>
</tr>
<tr>
<td></td>
<td>- Default value: true</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>glide.ui.m.clear_pasteboard_when_backgrounded</td>
<td>Clears the copy/paste clipboard when the ServiceNow application enters the background.</td>
</tr>
<tr>
<td></td>
<td>- Type: true</td>
</tr>
<tr>
<td></td>
<td>- Default value: false</td>
</tr>
<tr>
<td></td>
<td>- add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>glide.ui.max_calendar_duration</td>
<td>Maximum number of days that a single calendar report entry can display.</td>
</tr>
<tr>
<td></td>
<td>- Type: integer</td>
</tr>
<tr>
<td></td>
<td>- Default value: 90</td>
</tr>
<tr>
<td></td>
<td>- Range of possible values: 90 to 400</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>glide.ui.max_calendar_records</td>
<td>Maximum number of records saved in a calendar report.</td>
</tr>
<tr>
<td></td>
<td>- Type: integer</td>
</tr>
<tr>
<td></td>
<td>- Default value if the property is not configured: 10,000</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>glide.ui.m_agents</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: iphone, android_phone, IEMobile, Windows Phone, iPod, Windows CE, BlackBerry, BB10</td>
</tr>
<tr>
<td></td>
<td>• Location: System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.ui.max_ref_dropdown</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 25</td>
</tr>
<tr>
<td></td>
<td>• Location: System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.ui.mobile_agents</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: iPod, Windows CE, BlackBerry, Android, Opera Mini, IEMobile, Windows Phone, iphone</td>
</tr>
<tr>
<td></td>
<td>• Location: System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.ui.nav.stripe.select.maxchars</td>
<td>Numerical character limit for list menu choices within the nav stripe. The nav stripe displays at the top of the page when using UI11.</td>
</tr>
<tr>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: none</td>
</tr>
<tr>
<td></td>
<td>• Location: add the property</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</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.  
  - Type: true | false  
  - Default value: false  
  - Location: System Properties > UI Properties  
  If set to false, the administrator can override the system setting for a specific field by adding the `readonly_clickthrough=true` attribute to the dictionary entry. |
| 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 this property is set to false, field styles in only the Task table are used. If this property is set to true, the calendar first uses field styles from the table 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  
  - Add a system property |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.ui.section508</td>
<td>Enables (true) or disables (false) rendering of alternate text in place of images.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td>glide.ui.show_live_feed_activity</td>
<td>Enables (true) or disables (false) live feed for a record in the activity formatter.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td>glide.ui.show_template_bar.&lt;TABLENAME&gt;</td>
<td>Controls whether the template bar can be displayed on the specified table. For example:</td>
</tr>
<tr>
<td></td>
<td>glide.ui.show_template_bar.incident = false</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td>glide.ui.session_timeout</td>
<td>Sets the session timeout, in minutes.</td>
</tr>
<tr>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td>glide.ui.stream_icon.&lt;TABLENAME&gt;</td>
<td>Toggles the displaying of the activity stream button on the specified table. For example:</td>
</tr>
<tr>
<td></td>
<td>glide.ui.stream_icon.hr_case = true</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td>glide.ui.table.labels</td>
<td>Controls whether the system uses verbose labels for table names (true) or literal table names (false).</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td>glide.ui.tablet_enabled</td>
<td>Enables (true) or disables (false) the tablet UI.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>glide.ui.tablet_agents</td>
<td>Uses the tablet UI if one of these strings (comma-separated) appears in the browser user_agent</td>
</tr>
<tr>
<td></td>
<td>header</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: ipad, android_tablet</td>
</tr>
<tr>
<td></td>
<td>• Location: System Properties &gt; Tablet UI Properties</td>
</tr>
<tr>
<td>glide.ui.tablet.title</td>
<td>Displays a brief page title for tablet UI.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: ServiceNow</td>
</tr>
<tr>
<td></td>
<td>• Location: System Properties &gt; Tablet UI Properties</td>
</tr>
<tr>
<td>glide.ui.tablet.title.ios_webapp</td>
<td>Displays the specified text as the default home screen icon label used in iOS version 6 and later.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: ServiceNow</td>
</tr>
<tr>
<td></td>
<td>• Location: System Properties &gt; Tablet UI Properties</td>
</tr>
<tr>
<td>glide.ui.task.insert</td>
<td>Enables (true) or disables (false) the use of Insert and Insert and Stay options on tables</td>
</tr>
<tr>
<td></td>
<td>derived from Task (such as Incident, Change, and Problem).</td>
</tr>
<tr>
<td></td>
<td>• Type: true</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>glide.ui.textarea.character_counter</td>
<td>When true, displays a count of available characters for journal and multi-line text fields.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</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>glide.ui.textarea_initial_rows</td>
<td>Sets the number of rows initially displayed for multiline form elements. When the element is</td>
</tr>
<tr>
<td></td>
<td>selected for editing, it is expanded. Set this value to 0 or blank to ignore this property.</td>
</tr>
<tr>
<td></td>
<td>This functionality is used to conserve space on a form when multiline elements take up too</td>
</tr>
<tr>
<td></td>
<td>much space on forms.</td>
</tr>
<tr>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 0</td>
</tr>
<tr>
<td></td>
<td>• Location: System Property (sys_properties) table</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| 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 to the 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 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 |
<p>| Name                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.xmlprocessor.use_unload_format</td>
<td>Enables (true) or disables (false) unloading the XML using the display_value format. To unload using this format, add the parameter <code>useUnloadFormat=true</code> to the request URL.</td>
</tr>
<tr>
<td></td>
<td>- Type: true</td>
</tr>
<tr>
<td></td>
<td>- Default value: false</td>
</tr>
<tr>
<td></td>
<td>- Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>glide.wsdl.show_nillable</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>- Type: true</td>
</tr>
<tr>
<td></td>
<td>- Default value: false</td>
</tr>
<tr>
<td></td>
<td>- Location: add to the System Property (sys_properties) table</td>
</tr>
<tr>
<td>google.maps.auto_close</td>
<td>If true, automatically closes the current info window before opening a new one. Clear the check box to allow multiple pop-up windows to remain open at once.</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: [System Properties &gt; Google Maps]</td>
</tr>
<tr>
<td>google.maps.client</td>
<td>Client ID for Google Maps API for Business. This is the client ID authorizing 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.</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: [System Properties &gt; Google Maps]</td>
</tr>
<tr>
<td>google.maps.key</td>
<td>Map key from Google, tied to the URL of the server. This is the private key authorizing development use of Google Maps.</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; Google Maps]</td>
</tr>
<tr>
<td>google.maps.latitude</td>
<td>Starting latitude of the map. This value determines the starting latitude 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: [System Properties &gt; Google Maps]</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>google.maps.longitude</td>
<td>Starting longitude of the map. This value determines the starting longitude displayed in Google Maps.</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: [System Properties &gt; Google Maps]</td>
</tr>
<tr>
<td>google.maps.max_items</td>
<td>Maximum number of items to display on the map. This setting determines how many icons can be displayed on a 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: [System Properties &gt; Google Maps]</td>
</tr>
<tr>
<td>google.maps.table</td>
<td>Table used by the map. This setting names the table containing the name, longitude, and latitude fields.</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: [System Properties &gt; Google Maps]</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: [System Properties &gt; Google Maps]</td>
</tr>
<tr>
<td>help.base.default</td>
<td>(Context-Sensitive Help plugin) Sets the base URL for help contexts in which ServiceNow wiki is false and an absolute URL is not specified.</td>
</tr>
<tr>
<td></td>
<td>- Type: string</td>
</tr>
<tr>
<td></td>
<td>- Location: System Property (sys_properties) table</td>
</tr>
<tr>
<td>help.base.servicenow</td>
<td>(Context-Sensitive Help plugin) Sets the base URL for help contexts in which ServiceNow wiki is true</td>
</tr>
<tr>
<td></td>
<td>- Type: string</td>
</tr>
<tr>
<td></td>
<td>- Location: System Property (sys_properties) table</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>mid.server.rba_debug_powershell</td>
<td>Enables probe-level debugging for PowerShell probes. With this property enabled, PowerShell probes write detailed activity information to the MID Server log.</td>
</tr>
<tr>
<td></td>
<td>- Type: true</td>
</tr>
<tr>
<td></td>
<td>- Default value: false</td>
</tr>
<tr>
<td></td>
<td>- Location: Orchestration &gt; MID Server Properties</td>
</tr>
<tr>
<td>password_reset.activity_monitor.incident_threshold</td>
<td>Determines the maximum number of lockouts before an alert is issued.</td>
</tr>
<tr>
<td></td>
<td>- Type: integer</td>
</tr>
<tr>
<td></td>
<td>- Default value: 10 (lockouts)</td>
</tr>
<tr>
<td></td>
<td>- Location: Password Reset &gt; Properties</td>
</tr>
<tr>
<td>password_reset.activity_monitor.incident_window</td>
<td>Determines the amount of time that is used for recording and counting the number of user lockouts.</td>
</tr>
<tr>
<td></td>
<td>- Type: integer</td>
</tr>
<tr>
<td></td>
<td>- Default value: 60 (minutes)</td>
</tr>
<tr>
<td></td>
<td>- Location: Password Reset &gt; Properties</td>
</tr>
<tr>
<td>password_reset.captcha.ignore</td>
<td>Enables and disables CAPTCHA functionality.</td>
</tr>
<tr>
<td></td>
<td>- Type: true</td>
</tr>
<tr>
<td></td>
<td>- Default value: false</td>
</tr>
<tr>
<td></td>
<td>- Location: Password Reset &gt; Properties</td>
</tr>
<tr>
<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.</td>
</tr>
<tr>
<td>password_reset.qa.num_enroll</td>
<td>Specifies the number of questions a user has to select and answer to be enrolled in the password reset program.</td>
</tr>
<tr>
<td></td>
<td>- Type: integer</td>
</tr>
<tr>
<td></td>
<td>- Default value: 5 (questions)</td>
</tr>
<tr>
<td></td>
<td>- Location: Password Reset &gt; Properties</td>
</tr>
<tr>
<td></td>
<td>Note: This security question property can be overridden by adding a value for the num_enroll parameter in a security question verification.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>password_reset.qa.num_reset</strong></td>
<td>Specifies the number of questions a user has to answer to verify their identity during the password reset process.</td>
</tr>
<tr>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 3 (questions)</td>
</tr>
<tr>
<td></td>
<td>• Possible values: integers that are less than the number specified for the <strong>num_enroll</strong> property.</td>
</tr>
<tr>
<td></td>
<td>• Location: <strong>Password Reset &gt; Properties</strong></td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>This security question property can be overridden by adding a value for the <strong>num_reset</strong> parameter in a security question verification.</td>
</tr>
<tr>
<td><strong>password_reset.request.max_attempt</strong></td>
<td>Determines the number of password reset attempts a user has before they are locked out for a period determined by the value in <strong>max_attempt_window</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 3 (attempts)</td>
</tr>
<tr>
<td></td>
<td>• Location: <strong>Password Reset &gt; Properties</strong></td>
</tr>
<tr>
<td><strong>password_reset.request.max_attempt_window</strong></td>
<td>Determines how long a user is locked out or prevented from changing their password after trying the maximum number of times.</td>
</tr>
<tr>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 1440 (minutes)</td>
</tr>
<tr>
<td></td>
<td>• Location: <strong>Password Reset &gt; Properties</strong></td>
</tr>
<tr>
<td><strong>password_reset.request.retry_window</strong></td>
<td>Determines length of time before the count for password reset attempts refreshes.</td>
</tr>
<tr>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 1440 (minutes)</td>
</tr>
<tr>
<td></td>
<td>• Location: <strong>Password Reset &gt; Properties</strong></td>
</tr>
<tr>
<td><strong>password_reset.request.success_window</strong></td>
<td>Determines how long a user is locked out after they have successfully reset their password.</td>
</tr>
<tr>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 10 (minutes)</td>
</tr>
<tr>
<td></td>
<td>• Location: <strong>Password Reset &gt; Properties</strong></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>password_reset.sms.default_complexity</td>
<td>Specifies the number of characters required for a user to reset their password.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This SMS code property can be overridden by adding a value for the complexity parameter in an SMS code verification.</td>
</tr>
<tr>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 4 (digits)</td>
</tr>
<tr>
<td></td>
<td>• Location: Password Reset &gt; Properties</td>
</tr>
<tr>
<td>password_reset.sms.expiry</td>
<td>Determines the amount of time, in minutes, until the SMS code sent to the user expires.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This SMS code property can be overridden by adding a value for the expiry parameter in an SMS code verification.</td>
</tr>
<tr>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 5 (minutes)</td>
</tr>
<tr>
<td></td>
<td>• Location: Password Reset &gt; Properties</td>
</tr>
<tr>
<td>password_reset.sms.max_per_day</td>
<td>Determines 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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This SMS code property can be overridden by adding a value for the max_per_day parameter in an SMS code verification.</td>
</tr>
<tr>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 10 (per day)</td>
</tr>
<tr>
<td></td>
<td>• Location: Password Reset &gt; Properties</td>
</tr>
<tr>
<td>password_reset.sms.pause_window</td>
<td>Determines the amount of time that needs to pass before another SMS code can be sent to a user.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This SMS code property can be overridden by adding a value for the pause_window parameter in an SMS code verification.</td>
</tr>
<tr>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 2 (minutes)</td>
</tr>
<tr>
<td></td>
<td>• Location: Password Reset &gt; Properties</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>password_reset.wf.refresh_rate</td>
<td>Determines how often to check status of the workflow. Represented in the password reset process progress bar.</td>
</tr>
<tr>
<td></td>
<td>- Type: integer</td>
</tr>
<tr>
<td></td>
<td>- Default value: 90000 (milliseconds)</td>
</tr>
<tr>
<td></td>
<td>- Location: Password Reset &gt; Properties</td>
</tr>
<tr>
<td>password_reset.wf.timeout</td>
<td>Determines 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.</td>
</tr>
<tr>
<td></td>
<td>- Type: integer</td>
</tr>
<tr>
<td></td>
<td>- Default value: 500 (milliseconds)</td>
</tr>
<tr>
<td></td>
<td>- Location: Password Reset &gt; Properties</td>
</tr>
<tr>
<td>sam.install_deletion_deadline</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>- Type: integer</td>
</tr>
<tr>
<td></td>
<td>- Default value: 7</td>
</tr>
<tr>
<td></td>
<td>- Location: System Property (sys_properties) table</td>
</tr>
<tr>
<td>tablet.header.text</td>
<td>Text that appears on the right-hand side of the tablet UI header.</td>
</tr>
<tr>
<td></td>
<td>- Type: string</td>
</tr>
<tr>
<td></td>
<td>- Default value: ServiceNow</td>
</tr>
<tr>
<td></td>
<td>- Location: System Properties &gt; Tablet UI Properties</td>
</tr>
<tr>
<td>tablet.footer.text</td>
<td>Text that appears on the footer of the tablet UI.</td>
</tr>
<tr>
<td></td>
<td>- Type: string</td>
</tr>
<tr>
<td></td>
<td>- Default value: Copyright ServiceNow 2012</td>
</tr>
<tr>
<td></td>
<td>- Location: System Properties &gt; Tablet UI Properties</td>
</tr>
<tr>
<td>glide.bsm.map.style.text_color</td>
<td>Color of the text that appears under an unselected CI node.</td>
</tr>
<tr>
<td></td>
<td>- Type: color</td>
</tr>
<tr>
<td></td>
<td>- Default value: Black</td>
</tr>
<tr>
<td></td>
<td>- Location: BSM Map &gt; Map Properties</td>
</tr>
<tr>
<td>glide.bsm.map.style.selection_text_color</td>
<td>Color of the text that appears under a selected CI node.</td>
</tr>
<tr>
<td></td>
<td>- Type: color</td>
</tr>
<tr>
<td></td>
<td>- Default value: White</td>
</tr>
<tr>
<td></td>
<td>- Location: BSM Map &gt; Map Properties</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| 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.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, valid values 1 to 10  
  - Default value: 5  
  - 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 your users' 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.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.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 |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| glide.bsm.color.affect_neighbors          | Color of an affected neighbor node. When a node has a service issue, all the nodes that are dependent 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.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.task_threshold                  | Change the CI's 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.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.entry.loggedin.page_ess             | Specified 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.required.attribute.enabled          | Flag for enforcing required attributes (can't be null) during identification and reconciliation.  
  - Type: true | false  
  - Default value: true  
  - Location: System Properties (sys_properties) table.                                                                                 |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.class.upgrade.enabled</td>
<td>Flag for allowing class update during identification and reconciliation.</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 Properties (sys_properties) table.</td>
</tr>
<tr>
<td>glide.class.downgrade.enabled</td>
<td>Flag for allowing class downgrade during identification and reconciliation.</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 Properties (sys_properties) table.</td>
</tr>
<tr>
<td>glide.class.switch.enabled</td>
<td>Flag for allowing class switching during identification and reconciliation.</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 Properties (sys_properties) table.</td>
</tr>
<tr>
<td>glide.reconciliation.override.null</td>
<td>Flag for allowing or disallowing the update of an empty field by a lower priority data source.</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 Properties (sys_properties) table.</td>
</tr>
<tr>
<td>glide.identification_engine.skip_duplicates</td>
<td>Controls how identification processes a small set of duplicate CIs.</td>
</tr>
<tr>
<td></td>
<td>- When true: If the number of duplicate CIs is less than the threshold specified by <code>glide.identification_engine.skip_duplicates.threshold</code></td>
</tr>
<tr>
<td></td>
<td>- then one of the duplicate CIs is picked as a match and gets updated. The rest of the duplicate CIs are tagged as duplicates.</td>
</tr>
<tr>
<td></td>
<td>- When false: Matching a CI fails, and an error is logged.</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 Properties (sys_properties) table.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</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 what it is set to.  
- Type: integer  
- Default value: 5  
- Location: add to the System Properties (sys_properties) table. |
| Enable alert aggregation                                            | Enables aggregation of correlated alerts for services and alert groups.  
- Type: true | false  
- Default value: true  
- Location: Alert Aggregation and RCA > Properties |
| Enable 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 |
| Include CIs associated with business services, in alert aggregation  |  
- Type: true | false  
- Default value: true  
- 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 |
| 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 |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time interval (in seconds) criteria for grouping alerts</td>
<td>Interval that alerts must be created in, to be included in a group.</td>
</tr>
</tbody>
</table>
| **sa_analytics.rca.learner_group_interval_secs**                    | • Type: integer  
• Default value: 300  
• Range of possible values: 60-900  
• Location: Alert Aggregation and RCA > Properties |
| 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.                                                                                                                              |
| **sa_analytics.rca.learner_query_interval_secs**                    | • Type: integer  
• Default value: 86400  
• Range of possible values: 43200-86400  
• Location: Alert Aggregation and RCA > Properties |
| Confidence score % threshold, above which RCA correlated alert groups will be displayed 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.                                                   |
| **sa_analytics.rca.query_probability_threshold**                    | • Type: integer  
• Default value: 0  
• Range of possible values: 0-100  
• Location: Alert Aggregation and RCA > Properties |
| Alert severity threshold, above which alerts will be included in analysis | Only alerts with severity that is above the threshold are included in alert aggregations and root cause CI analysis.                                                                                   |
| **sa_analytics.alert.severity_threshold**                           | • Type: choice list  
• Default value: Info  
• Other possible values:  
  • Warning  
  • Minor  
  • Major  
  • Critical  
• Location: Alert Aggregation and RCA > Properties |
| Time unit to use for KPI values on the Benchmarks dashboard          | Options are Hours or Days                                                                                                                                                                               |
| **sn_bm_client.dashboard_display_unit**                             | • Type: choice list  
• Default value: Days  
• Location: System Property (sys_properties) table |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sn_chg_soc.change_soc_initial_limit</td>
<td>Define the number of change_request records to display on load of the Change Schedule.</td>
</tr>
<tr>
<td></td>
<td>• Type: Integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 40</td>
</tr>
<tr>
<td></td>
<td>• Location: System Property (sys_properties) table</td>
</tr>
<tr>
<td>sn_chg_soc.change_soc_scroll_load_limit</td>
<td>Define the number of change_request records to display as the Change Schedule is scrolled.</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 Property (sys_properties) table</td>
</tr>
<tr>
<td>sn_chg_soc.change_soc_total_limit</td>
<td>Define the total number of change_request records that can be displayed on a Change Schedule.</td>
</tr>
<tr>
<td></td>
<td>• Type: Integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 1000</td>
</tr>
<tr>
<td></td>
<td>• Location: System Property (sys_properties) table</td>
</tr>
<tr>
<td>sn_chg_soc.landing_page.pinned_notification</td>
<td>Show a message when pin or unpin a change schedule.</td>
</tr>
<tr>
<td></td>
<td>• Type: String</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>sn_chg_soc.schedule_window_days</td>
<td>Define 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.</td>
</tr>
<tr>
<td></td>
<td>• Type: Integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 30</td>
</tr>
<tr>
<td></td>
<td>• Location: System Property (sys_properties) table</td>
</tr>
</tbody>
</table>

**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 [Developer Portal](https://developer.servicenow.com/). Some properties in the system are not visible in an instance by default and must be added to the System Property (sys_properties) table. You can add a system property if a feature requires the addition of the 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 gs.getProperty() method, treat the results as strings. For example, a true</td>
</tr>
<tr>
<td>Ignore cache</td>
<td>Set this option to true to refresh the cache before processing the property. The cache stores commonly used items in memory such as forms and UI elements. Typically, you only ignore the cache if the system property depends upon a dynamic change on the form, and you want to ensure that the property uses the current value rather than a cached value.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</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 ServiceNow 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 ServiceNow 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.

| 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. | 10 |

**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.

**Note:** In the absence of known database issues stemming from large join counts, this parameter should remain unchanged.

**Tables and classes**

Administrators can use the schema map, Tables module, or the system dictionary to determine which system tables extend other tables.

**Tables that are extensions of other tables**

<table>
<thead>
<tr>
<th>Table Name</th>
<th>Label</th>
<th>Extension of</th>
<th>Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>ast_lease</td>
<td>Lease</td>
<td>ast_contract</td>
<td>Contract</td>
</tr>
<tr>
<td>ast_license_adobe</td>
<td>Adobe Software License</td>
<td>ast_license_base</td>
<td>Base License Table</td>
</tr>
<tr>
<td>ast_license_generic</td>
<td>Generic Software License</td>
<td>ast_license_base</td>
<td>Base License Table</td>
</tr>
<tr>
<td>ast_license_msft</td>
<td>Microsoft Software License</td>
<td>ast_license_base</td>
<td>Base License Table</td>
</tr>
<tr>
<td>ast_license_symantec</td>
<td>Symantec Software License</td>
<td>ast_license_base</td>
<td>Base License Table</td>
</tr>
<tr>
<td>ast_service</td>
<td>Service Contract</td>
<td>ast_contract</td>
<td>Contract</td>
</tr>
<tr>
<td>ast_warranty</td>
<td>Warranty</td>
<td>ast_contract</td>
<td>Contract</td>
</tr>
<tr>
<td>bsm_action</td>
<td>BSM Map Actions</td>
<td>diagrammer_action</td>
<td>Diagrammer Actions</td>
</tr>
<tr>
<td>Table Name</td>
<td>Label</td>
<td>Extension of</td>
<td>Label</td>
</tr>
<tr>
<td>------------</td>
<td>-------</td>
<td>--------------</td>
<td>-------</td>
</tr>
<tr>
<td>catalog_script_client</td>
<td>Catalog Client Scripts</td>
<td>sys_script_client</td>
<td>Client Script</td>
</tr>
<tr>
<td>catalog_ui_policy</td>
<td>Catalog UI Policy</td>
<td>sys_ui_policy</td>
<td>UI Policy</td>
</tr>
<tr>
<td>catalog_ui_policy_action</td>
<td>Catalog UI Policy Action</td>
<td>sys_ui_policy_action</td>
<td>UI Policy Action</td>
</tr>
<tr>
<td>change_phase</td>
<td>Change Phase</td>
<td>task</td>
<td>Task</td>
</tr>
<tr>
<td>change_request</td>
<td>Change Request</td>
<td>task</td>
<td>Task</td>
</tr>
<tr>
<td>change_request_imac</td>
<td>IMAC</td>
<td>change_request</td>
<td>Change Request</td>
</tr>
<tr>
<td>change_task</td>
<td>Change Task</td>
<td>task</td>
<td>Task</td>
</tr>
<tr>
<td>cmdb_ci.acc</td>
<td>Accessory</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_aix_server</td>
<td>AIX Server</td>
<td>cmdb_ci_unix_server</td>
<td>Unix Server</td>
</tr>
<tr>
<td>cmdb_ci_apache_web_server</td>
<td>Apache Web Server</td>
<td>cmdb_ci_web_server</td>
<td>Web Server</td>
</tr>
<tr>
<td>cmdb_ci_appl</td>
<td>Application</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_application_software</td>
<td>Application Software</td>
<td>cmdb_ci_spkg</td>
<td>Software</td>
</tr>
<tr>
<td>cmdb_ci_app_server</td>
<td>Application Server</td>
<td>cmdb_ci_appl</td>
<td>Application</td>
</tr>
<tr>
<td>cmdb_ci_app_server_domino</td>
<td>Domino</td>
<td>cmdb_ci_app_server</td>
<td>Application Server</td>
</tr>
<tr>
<td>cmdb_ci_app_server_java</td>
<td>Java Server</td>
<td>cmdb_ci_app_server</td>
<td>Application Server</td>
</tr>
<tr>
<td>cmdb_ci_app_server_jboss</td>
<td>Jboss</td>
<td>cmdb_ci_app_server</td>
<td>Application Server</td>
</tr>
<tr>
<td>cmdb_ci_app_server_tomcat</td>
<td>Tomcat</td>
<td>cmdb_ci_app_server</td>
<td>Application Server</td>
</tr>
<tr>
<td>cmdb_ci_app_server_weblogic</td>
<td>BEA Weblogic</td>
<td>cmdb_ci_app_server</td>
<td>Application Server</td>
</tr>
<tr>
<td>cmdb_ci_app_server_websphere</td>
<td>IBM Websphere</td>
<td>cmdb_ci_app_server</td>
<td>Application Server</td>
</tr>
<tr>
<td>cmdb_ci_business_process</td>
<td>Business Process</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_circuit</td>
<td>Circuit</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_cluster</td>
<td>Cluster</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_cluster_node</td>
<td>Cluster Node</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_cluster_resource</td>
<td>Cluster Resource</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_cluster_vip</td>
<td>Cluster Virtual IP</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_comm</td>
<td>Communication Device</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_computer</td>
<td>Computer</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_computer_room</td>
<td>Computer Room</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_crac</td>
<td>Computer Room AC</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_database</td>
<td>Database</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_datacenter</td>
<td>Data Center</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_db_catalog</td>
<td>Database Catalog</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_db_db2_catalog</td>
<td>DB2 Catalog</td>
<td>cmdb_ci_db_catalog</td>
<td>Database Catalog</td>
</tr>
<tr>
<td>cmdb_ci_db_db2_instance</td>
<td>DB2 Instance</td>
<td>cmdb_ci_db_instance</td>
<td>Database Instance</td>
</tr>
<tr>
<td>cmdb_ci_db_instance</td>
<td>Database Instance</td>
<td>cmdb_ci_appl</td>
<td>Application</td>
</tr>
<tr>
<td>cmdb_ci_db_mssql_catalog</td>
<td>MSFT SQL Catalog</td>
<td>cmdb_ci_db_catalog</td>
<td>Database Catalog</td>
</tr>
<tr>
<td>Table Name</td>
<td>Label</td>
<td>Extension of</td>
<td>Label</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------------------</td>
<td>-----------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>cmdb_ci_db_mssql_instance</td>
<td>MSFT SQL Instance</td>
<td>cmdb_ci_db_instance</td>
<td>Database Instance</td>
</tr>
<tr>
<td>cmdb_ci_db_mysql_catalog</td>
<td>MySQL Catalog</td>
<td>cmdb_ci_db_catalog</td>
<td>Database Catalog</td>
</tr>
<tr>
<td>cmdb_ci_db_mysql_instance</td>
<td>MySQL Instance</td>
<td>cmdb_ci_db_instance</td>
<td>Database Instance</td>
</tr>
<tr>
<td>cmdb_ci_db_ora_catalog</td>
<td>Oracle Catalog</td>
<td>cmdb_ci_db_catalog</td>
<td>Database Catalog</td>
</tr>
<tr>
<td>cmdb_ci_db_ora_instance</td>
<td>Oracle Instance</td>
<td>cmdb_ci_db_instance</td>
<td>Database Instance</td>
</tr>
<tr>
<td>cmdb_ci_db_syb_catalog</td>
<td>Sybase Catalog</td>
<td>cmdb_ci_db_catalog</td>
<td>Database Catalog</td>
</tr>
<tr>
<td>cmdb_ci_db_syb_instance</td>
<td>Sybase Instance</td>
<td>cmdb_ci_db_instance</td>
<td>Database Instance</td>
</tr>
<tr>
<td>cmdb_ci_desktop_software</td>
<td>Desktop Software</td>
<td>cmdb_ci_spkg</td>
<td>Software</td>
</tr>
<tr>
<td>cmdb_ci_directory_server</td>
<td>Directory Server</td>
<td>cmdb_ci_infra_service</td>
<td>Infrastructure Service</td>
</tr>
<tr>
<td>cmdb_ci_disk</td>
<td>Disk</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_email_server</td>
<td>Email Server</td>
<td>cmdb_ci_infra_service</td>
<td>Infrastructure Service</td>
</tr>
<tr>
<td>cmdb_ci_esx_server</td>
<td>ESXi Server</td>
<td>cmdb_ci_server</td>
<td>Server</td>
</tr>
<tr>
<td>cmdb_ci_file_system</td>
<td>File System</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_file_system_nfs</td>
<td>NFS File System</td>
<td>cmdb_ci_file_system</td>
<td>File System</td>
</tr>
<tr>
<td>cmdb_ci_file_system_smb</td>
<td>SMB File System</td>
<td>cmdb_ci_file_system</td>
<td>File System</td>
</tr>
<tr>
<td>cmdb_ci_ftp_server</td>
<td>FTP Server</td>
<td>cmdb_ci_infra_service</td>
<td>Infrastructure Service</td>
</tr>
<tr>
<td>cmdb_ci_group</td>
<td>Group</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_hpx_server</td>
<td>HPUX Server</td>
<td>cmdb_ci_unix_server</td>
<td>Unix Server</td>
</tr>
<tr>
<td>cmdb_ci_infra_service</td>
<td>Infrastructure Service</td>
<td>cmdb_ci_appl</td>
<td>Application</td>
</tr>
<tr>
<td>cmdb_ci_infra_service ldap</td>
<td>LDAP Service</td>
<td>cmdb_ci_infra_service</td>
<td>Infrastructure Service</td>
</tr>
<tr>
<td>cmdb_ci_inf_software</td>
<td>Infrastructure Software</td>
<td>cmdb_ci_spkg</td>
<td>Software</td>
</tr>
<tr>
<td>cmdb_ci_ip_device</td>
<td>IP Device</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_ip_network</td>
<td>IP Network</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_ip_phone</td>
<td>IP Phone</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_ip_router</td>
<td>IP Router</td>
<td>cmdb_ci_netgear</td>
<td>Network Gear</td>
</tr>
<tr>
<td>cmdb_ci_ip_server</td>
<td>IP Server</td>
<td>cmdb_ci_infra_service</td>
<td>Infrastructure Service</td>
</tr>
<tr>
<td>cmdb_ci_ip_service</td>
<td>IP Service</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_ip_switch</td>
<td>IP Switch</td>
<td>cmdb_ci_netgear</td>
<td>Network Gear</td>
</tr>
<tr>
<td>cmdb_ci_iplanet_web_server</td>
<td>iPlanet Web Server</td>
<td>cmdb_ci_web_server</td>
<td>Web Server</td>
</tr>
<tr>
<td>cmdb_ci_linux_server</td>
<td>Linux Server</td>
<td>cmdb_ci_server</td>
<td>Server</td>
</tr>
<tr>
<td>cmdb_ci_mainframe</td>
<td>IBM Mainframe</td>
<td>cmdb_ci_server</td>
<td>Server</td>
</tr>
<tr>
<td>cmdb_ci_mainframe_lpar</td>
<td>IBM Mainframe LPAR</td>
<td>cmdb_ci_server</td>
<td>Server</td>
</tr>
<tr>
<td>cmdb_ci_microsoft_iis_web_server</td>
<td>IIS Web Server</td>
<td>cmdb_ci_web_server</td>
<td>Web Server</td>
</tr>
<tr>
<td>cmdb_ci_msd</td>
<td>Storage Device</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_netgear</td>
<td>Network Gear</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_netware_server</td>
<td>Netware Server</td>
<td>cmdb_ci_server</td>
<td>Server</td>
</tr>
<tr>
<td>cmdb_ci_network_adapter</td>
<td>Network Adapter</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>Table Name</td>
<td>Label</td>
<td>Extension of</td>
<td>Label</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------------------</td>
<td>-----------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>cmdb_ci_net_traffic</td>
<td>Network Traffic</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_nginx_web_server</td>
<td>NGINX Web Server</td>
<td>cmdb_ci_web_server</td>
<td>Web Server</td>
</tr>
<tr>
<td>cmdb_ci_osx_server</td>
<td>OS/X Server</td>
<td>cmdb_ci_server</td>
<td>Server</td>
</tr>
<tr>
<td>cmdb_ci_patches</td>
<td>Patch</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_pdu</td>
<td>PDU</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_pdu_outlet</td>
<td>Outlet</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_peripheral</td>
<td>Computer Peripheral</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_printer</td>
<td>Printer</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_print_queue</td>
<td>Print Queue</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_rack</td>
<td>Rack</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_service</td>
<td>Business Service</td>
<td>cmdb_ci_computer</td>
<td>Computer</td>
</tr>
<tr>
<td>cmdb_ci_snc_component</td>
<td>SNC Component</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_solaris_server</td>
<td>Solaris Server</td>
<td>cmdb_ci_unix_server</td>
<td>Unix Server</td>
</tr>
<tr>
<td>cmdb_ci_spkg</td>
<td>Software</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_tomcat_connector</td>
<td>Tomcat Connector</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_unix_daemon</td>
<td>Unix Daemon</td>
<td>cmdb_ci_ip_service</td>
<td>IP Service</td>
</tr>
<tr>
<td>cmdb_ci_unix_server</td>
<td>Unix Server</td>
<td>cmdb_ci_server</td>
<td>Server</td>
</tr>
<tr>
<td>cmdb_ci_ups</td>
<td>UPS</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_ups_alarm</td>
<td>UPS Alarm</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_ups_bypass</td>
<td>UPS Bypass</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_ups_input</td>
<td>UPS Input</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_ups_output</td>
<td>UPS Output</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_vm</td>
<td>Virtual Machine</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_vm_parallels</td>
<td>Parallels</td>
<td>cmdb_ci_vm</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>cmdb_ci_vm_vmware</td>
<td>VMware</td>
<td>cmdb_ci_vm</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>cmdb_ci_vm_zones</td>
<td>Zones</td>
<td>cmdb_ci_vm</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>cmdb_ci_vpn</td>
<td>Virtual Private Network</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_websphere_cell</td>
<td>Websphere Cell</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_ci_web_application</td>
<td>Web Application</td>
<td>cmdb_ci_appl</td>
<td>Application</td>
</tr>
<tr>
<td>cmdb_ci_web_server</td>
<td>Web Server</td>
<td>cmdb_ci_infra_service</td>
<td>Infrastructure Service</td>
</tr>
<tr>
<td>cmdb_ci_web_service</td>
<td>Web Service</td>
<td>cmdb_ci_appl</td>
<td>Application</td>
</tr>
<tr>
<td>cmdb_ci_web_site</td>
<td>Web Site</td>
<td>cmdb_ci_appl</td>
<td>Application</td>
</tr>
<tr>
<td>cmdb_ci_windows_service</td>
<td>Windows Service</td>
<td>cmdb_ci_ip_service</td>
<td>IP Service</td>
</tr>
<tr>
<td>cmdb_ci_win_cluster</td>
<td>Windows Cluster</td>
<td>cmdb_ci_cluster</td>
<td>Cluster</td>
</tr>
<tr>
<td>cmdb_ci_win_cluster_node</td>
<td>Windows Cluster Node</td>
<td>cmdb_ci_cluster_node</td>
<td>Cluster Node</td>
</tr>
<tr>
<td>Table Name</td>
<td>Label</td>
<td>Extension of</td>
<td>Label</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------------------------</td>
<td>-----------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>cmdb_ci_win_cluster_resource</td>
<td>Windows Cluster Resource</td>
<td>cmdb_ci_cluster_resource</td>
<td>Cluster Resource</td>
</tr>
<tr>
<td>cmdb_ci_win_server</td>
<td>Windows Server</td>
<td>cmdb_ci_server</td>
<td>Server</td>
</tr>
<tr>
<td>cmdb_ci_zone</td>
<td>Zone</td>
<td>cmdb_ci</td>
<td>Configuration Item</td>
</tr>
<tr>
<td>cmdb_metric_cpu</td>
<td>CI CPU Metrics</td>
<td>cmdb_metric</td>
<td>CI Metric</td>
</tr>
<tr>
<td>cmdb_metric_db_connection</td>
<td>DB Connection Metric</td>
<td>cmdb_metric</td>
<td>CI Metric</td>
</tr>
<tr>
<td>cmdb_metric_errors</td>
<td>Errors Logged</td>
<td>cmdb_metric</td>
<td>CI Metric</td>
</tr>
<tr>
<td>cmdb_metric_events_processed</td>
<td>Events Processed</td>
<td>cmdb_metric</td>
<td>CI Metric</td>
</tr>
<tr>
<td>cmdb_metric_event_logs</td>
<td>Events Logged</td>
<td>cmdb_metric</td>
<td>CI Metric</td>
</tr>
<tr>
<td>cmdb_metric_java</td>
<td>CI Java Metric</td>
<td>cmdb_metric</td>
<td>CI Metric</td>
</tr>
<tr>
<td>cmdb_metric_linux_memory</td>
<td>Linux Memory Metrics</td>
<td>cmdb_metric</td>
<td>CI Metric</td>
</tr>
<tr>
<td>cmdb_metric_load</td>
<td>CI Load Metrics</td>
<td>cmdb_metric</td>
<td>CI Metric</td>
</tr>
<tr>
<td>cmdb_metric_logs</td>
<td>CI Log Count</td>
<td>cmdb_metric</td>
<td>CI Metric</td>
</tr>
<tr>
<td>cmdb_metric_mysql_statement</td>
<td>MySQL Metrics</td>
<td>cmdb_metric</td>
<td>CI Metric</td>
</tr>
<tr>
<td>cmdb_metric_oracle</td>
<td>CI Oracle Metrics</td>
<td>cmdb_metric</td>
<td>CI Metric</td>
</tr>
<tr>
<td>cmdb_metric_partition</td>
<td>Partition Read/Write Statistics</td>
<td>cmdb_metric</td>
<td>CI Metric</td>
</tr>
<tr>
<td>cmdb_metric_semaphore</td>
<td>CI Semaphore Metrics</td>
<td>cmdb_metric</td>
<td>CI Metric</td>
</tr>
<tr>
<td>cmdb_metric_service_now</td>
<td>CI Service-Now Metrics</td>
<td>cmdb_metric</td>
<td>CI Metric</td>
</tr>
<tr>
<td>cmdb_metric_sql</td>
<td>SQL Response Metrics</td>
<td>cmdb_metric</td>
<td>CI Metric</td>
</tr>
<tr>
<td>cmdb_metric_transaction</td>
<td>CI Transaction Metrics</td>
<td>cmdb_metric</td>
<td>CI Metric</td>
</tr>
<tr>
<td>discovery_probes_multi</td>
<td>Multiprobe</td>
<td>discovery_probes</td>
<td>Probe</td>
</tr>
<tr>
<td>discovery_probes_snmp</td>
<td>SNMP Probe</td>
<td>discovery_probes</td>
<td>Probe</td>
</tr>
<tr>
<td>discovery_probes_wmi</td>
<td>WMI Probe</td>
<td>discovery_probes</td>
<td>Probe</td>
</tr>
<tr>
<td>ecc_agent_counter_metric</td>
<td>ECC Agent Counter Metric</td>
<td>ecc_agent_metric</td>
<td>ECC Agent Metric</td>
</tr>
<tr>
<td>ecc_agent_memory_metric</td>
<td>ECC Agent Memory Metric</td>
<td>ecc_agent_metric</td>
<td>ECC Agent Metric</td>
</tr>
<tr>
<td>ecc_agent_rgr_metric</td>
<td>ECC Agent RGR Metric</td>
<td>ecc_agent_metric</td>
<td>ECC Agent Metric</td>
</tr>
<tr>
<td>ecc_agent_scalar_metric</td>
<td>ECC Agent Scalar Metric</td>
<td>ecc_agent_metric</td>
<td>ECC Agent Metric</td>
</tr>
<tr>
<td>expert_panel_catalog_checkout</td>
<td>Catalog Checkout Panel</td>
<td>expert_panel</td>
<td>Wizard Panel</td>
</tr>
<tr>
<td>expert_panel_catalog_order</td>
<td>Catalog Order</td>
<td>expert_panel</td>
<td>Wizard Panel</td>
</tr>
<tr>
<td>expert_panel_knowledge</td>
<td>KB Viewer</td>
<td>expert_panel</td>
<td>Wizard Panel</td>
</tr>
<tr>
<td>expert_panel_template</td>
<td>Record Generator</td>
<td>expert_panel</td>
<td>Wizard Panel</td>
</tr>
<tr>
<td>expert_script_client</td>
<td>Wizard Client Script</td>
<td>sys_script_client</td>
<td>Client Script</td>
</tr>
<tr>
<td>expert_variable</td>
<td>Wizard Variable</td>
<td>question</td>
<td>Question</td>
</tr>
</tbody>
</table>

© 2019 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>Table Name</th>
<th>Label</th>
<th>Extension of</th>
<th>Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>import_log</td>
<td>Import Log</td>
<td>syslog</td>
<td>Log Entry</td>
</tr>
<tr>
<td>imp_computer</td>
<td>Computer</td>
<td>sys_import_set_row</td>
<td>Import Set Row</td>
</tr>
<tr>
<td>imp_location</td>
<td>Location</td>
<td>sys_import_set_row</td>
<td>Import Set Row</td>
</tr>
<tr>
<td>imp_notification</td>
<td>Notification</td>
<td>sys_import_set_row</td>
<td>Import Set Row</td>
</tr>
<tr>
<td>imp_user</td>
<td>User</td>
<td>sys_import_set_row</td>
<td>Import Set Row</td>
</tr>
<tr>
<td>incident</td>
<td>Incident</td>
<td>task</td>
<td>Task</td>
</tr>
<tr>
<td>item_option_new</td>
<td>Variable</td>
<td>question</td>
<td>Question</td>
</tr>
<tr>
<td>kb_submission</td>
<td>KB Submission</td>
<td>task</td>
<td>Task</td>
</tr>
<tr>
<td>ola</td>
<td>OLA</td>
<td>sla</td>
<td>SLA</td>
</tr>
<tr>
<td>plan_mysql</td>
<td>Plan MySQL</td>
<td>plan_execution</td>
<td>Plan Execution</td>
</tr>
<tr>
<td>plan_oracle</td>
<td>Plan Oracle</td>
<td>plan_execution</td>
<td>Plan Execution</td>
</tr>
<tr>
<td>problem</td>
<td>Problem</td>
<td>task</td>
<td>Task</td>
</tr>
<tr>
<td>process_step_approval</td>
<td>Approval Steps</td>
<td>process_step</td>
<td>Process Steps</td>
</tr>
<tr>
<td>release_phase</td>
<td>Release Phase</td>
<td>task</td>
<td>Task</td>
</tr>
<tr>
<td>release_task</td>
<td>Release Task</td>
<td>task</td>
<td>Task</td>
</tr>
<tr>
<td>scheduled_data_import</td>
<td>Scheduled Data Import</td>
<td>sysauto</td>
<td>Scheduled Job</td>
</tr>
<tr>
<td>scheduled_import_set</td>
<td>Scheduled Data Import</td>
<td>scheduled_data_import</td>
<td>Scheduled Data Import</td>
</tr>
<tr>
<td>sc_category_top_n</td>
<td>Dynamic Category</td>
<td>sc_category</td>
<td>Category</td>
</tr>
<tr>
<td>sc_cat_item_content</td>
<td>Content Item</td>
<td>sc_cat_item</td>
<td>Catalog Item</td>
</tr>
<tr>
<td>sc_cat_item_dt_approval</td>
<td>Execution Plan Approval Task</td>
<td>sc_cat_item_delivery_task</td>
<td>Execution Plan Task</td>
</tr>
<tr>
<td>sc_cat_item_guide</td>
<td>Order Guide</td>
<td>sc_cat_item</td>
<td>Catalog Item</td>
</tr>
<tr>
<td>sc_cat_item_producer</td>
<td>Record Producer</td>
<td>sc_cat_item</td>
<td>Catalog Item</td>
</tr>
<tr>
<td>sc_cat_item_wizard</td>
<td>Wizard Launcher</td>
<td>sc_cat_item</td>
<td>Catalog Item</td>
</tr>
<tr>
<td>sc_request</td>
<td>Request</td>
<td>task</td>
<td>Task</td>
</tr>
<tr>
<td>sc_req_item</td>
<td>Requested Item</td>
<td>task</td>
<td>Task</td>
</tr>
<tr>
<td>sc_task</td>
<td>Catalog Task</td>
<td>task</td>
<td>Task</td>
</tr>
<tr>
<td>survey_question_new</td>
<td>Question</td>
<td>question</td>
<td>Question</td>
</tr>
<tr>
<td>sysapproval_group</td>
<td>Group Approval</td>
<td>task</td>
<td>Task</td>
</tr>
<tr>
<td>sysauto_report</td>
<td>Scheduled Email of Report</td>
<td>sysauto</td>
<td>Scheduled Job</td>
</tr>
<tr>
<td>sysauto_script</td>
<td>Scheduled Script Extension</td>
<td>sysauto</td>
<td>Scheduled Job</td>
</tr>
<tr>
<td>sysauto_template</td>
<td>Scheduled Entity Generation</td>
<td>sysauto</td>
<td>Scheduled Job</td>
</tr>
<tr>
<td>sysevent_email_action</td>
<td>Email Notification</td>
<td>sysrule</td>
<td>Rule</td>
</tr>
<tr>
<td>sysevent_in_email_action</td>
<td>Inbound Email Actions</td>
<td>sysrule</td>
<td>Rule</td>
</tr>
<tr>
<td>sysevent_script_action</td>
<td>Script Action</td>
<td>sysrule</td>
<td>Rule</td>
</tr>
<tr>
<td>Table Name</td>
<td>Label</td>
<td>Extension of</td>
<td>Label</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------</td>
<td>--------------</td>
<td>------------</td>
</tr>
<tr>
<td>syslog_transaction</td>
<td>Transaction Log Entry</td>
<td>syslog</td>
<td>Rule</td>
</tr>
<tr>
<td>sysrule_approvals</td>
<td>Approval Rules</td>
<td>sysrule</td>
<td>Rule</td>
</tr>
<tr>
<td>sysrule_assignment</td>
<td>Assignment Rules</td>
<td>sysrule</td>
<td>Rule</td>
</tr>
<tr>
<td>sysrule_escalate</td>
<td>Service Level Agreement</td>
<td>sysrule</td>
<td>Rule</td>
</tr>
<tr>
<td>sysrule_escalate_am</td>
<td>Inactivity Monitor</td>
<td>sysrule_escalate</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>sysrule_view</td>
<td>View Rule</td>
<td>sysrule</td>
<td>Rule</td>
</tr>
<tr>
<td>ticket</td>
<td>Ticket</td>
<td>task</td>
<td>Task</td>
</tr>
<tr>
<td>var_dictionary</td>
<td>Variables</td>
<td>sys_dictionary</td>
<td>Dictionary</td>
</tr>
<tr>
<td>v_field_editor</td>
<td>Edit Field</td>
<td>v_field_creator</td>
<td>Create Field</td>
</tr>
<tr>
<td>v_table_editor</td>
<td>Edit Table</td>
<td>v_table_creator</td>
<td>Create Table</td>
</tr>
<tr>
<td>v_ws_creator</td>
<td>Create Web Service</td>
<td>v_table_creator</td>
<td>Create Table</td>
</tr>
<tr>
<td>v_ws_editor</td>
<td>Edit Web Service</td>
<td>v_ws_creator</td>
<td>Create Web Service</td>
</tr>
<tr>
<td>v_ws_field_creator</td>
<td>Create Web Service Field</td>
<td>v_field_creator</td>
<td>Create Field</td>
</tr>
<tr>
<td>v_ws_field_editor</td>
<td>Edit Web Service Field</td>
<td>v_field_editor</td>
<td>Edit Field</td>
</tr>
<tr>
<td>wf_activity_variable</td>
<td>Activity Variables</td>
<td>var_dictionary</td>
<td>Variables</td>
</tr>
<tr>
<td>wf_log</td>
<td>Workflow Log Entry</td>
<td>syslog</td>
<td>Log Entry</td>
</tr>
<tr>
<td>wf_variable</td>
<td>Workflow SC Variable</td>
<td>item_option_new</td>
<td>Variable</td>
</tr>
<tr>
<td>wf_workflow_schedule</td>
<td>Workflow Schedule</td>
<td>sysauto_script</td>
<td>Scheduled Script Execution</td>
</tr>
</tbody>
</table>

**Web proxy**

Several properties support Web proxy configuration.

**Note:** Set these properties in the System Properties [sys_properties] table.

**Proxy setup properties**

<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,</td>
</tr>
<tr>
<td></td>
<td>- Type: string</td>
<td>192.168.34.54</td>
</tr>
<tr>
<td></td>
<td>- Default value: none</td>
<td></td>
</tr>
<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>
</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 NTCredentials 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 NTCredentials 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 NTCredentials instead of UsernamePasswordCredentials (NTCredentials actually extends UsernamePasswordCredentials so you can use NTCredentials 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.

---

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<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>
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>
</table>
| glide.http.proxy_ntusername | Specify the username used to authenticate the proxy server with NTLM authentication.  
  - Type: string  
  - Default value: none | username |
| glide.http.proxy_ntpassword | Specify the password used to authenticate the proxy server with NTLM authentication.  
  - Type: string  
  - Default value: none | password |
| glide.http.proxy_nthost    | Specify the hostname used to authenticate the proxy server with NTLM authentication.  
  - Type: string  
  - Default value: none | nhost    |
| glide.http.proxy_ntdomain  | Specify the domain used to authenticate the proxy server with NTLM authentication.  
  - Type: string  
  - Default value: none | DOMAIN   |

### 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.
Bypass the proxy server

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.http.proxy_bypass_list</td>
<td>Specify 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.</td>
<td>127.0.0.1;*.internal.com;localhost</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>· Location: System Properties [sys_properties] table</td>
<td></td>
</tr>
<tr>
<td></td>
<td>127.0.0.1;*.internal.com;localhost</td>
<td></td>
</tr>
</tbody>
</table>

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>
<tbody>
<tr>
<td>Task (task)</td>
<td>· Incident (incident)</td>
</tr>
<tr>
<td></td>
<td>· Problem (problem)</td>
</tr>
<tr>
<td></td>
<td>· Change Request (change_request)</td>
</tr>
<tr>
<td>Configuration Item (cmdb_ci)</td>
<td>· Application (cmdb_ci_appl)</td>
</tr>
<tr>
<td></td>
<td>· Computer (cmdb_ci_computer)</td>
</tr>
<tr>
<td></td>
<td>· Database (cmdb_ci_database)</td>
</tr>
</tbody>
</table>
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.

**Note:** The concept of class refers specifically to Configuration Management Database (CMDB schema)-related tables that contain a Class column that indicates the type of child table for Configuration Item (CI). This concept does not apply to other tables in the Now Platform.

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. For example, the Service Contract (ast_service) table derives fields from the Contract (ast_contract) 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 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. For example, the Service Contract (ast_service) table only has four Dictionary records, which are not already defined in the Contract (ast_contract) table.

**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), Service Contract (ast_service), and Warranty (ast_warranty) tables. When you update a Service Contract record, the system also updates the same record in the Contract table.

### 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

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>
<tr>
<td>Control</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</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_.  
  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 (_). |
| Extends Table           | Select the table to extend. Extending a base table incorporates all the fields of the original table and creates system fields for the new table. You can extend tables that are marked as extensible if they are in the same scope or if they allow configuration from other scopes.  
  This option is available only when creating a table. |
| Application             | (Read only) Displays the application associated with this table. If you are working on an application or are creating a table 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. |
| Create module           | Select the check box and then complete the Add module to menu field to create a list module in the application menu.  
  This option is available only when creating a table. |
| Add module to menu      | Select an existing menu or select Create new and enter a new menu name. This option is available only when the Create module check box is selected. |

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>Column label</td>
<td>Define a unique label for the column. The label appears on list headers and form fields for the column. When you update the Column label field, the system also updates the label in the language file for the current language.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Type</td>
<td>(Mandatory) Define the field type for the column. See Introduction to Fields. To preserve existing data, only change fields between the same basic type (for example, Choice and String). 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>
<tr>
<td>Reference</td>
<td>Make the field into a reference field by entering the referenced table name.</td>
</tr>
<tr>
<td>Max length</td>
<td>(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.</td>
</tr>
</tbody>
</table>

**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.

**Note:**
- You can only change this value if the type of the field is String. Changes for any other type of field are ignored.
- Users on an Oracle instance cannot increase the maximum length of a string field to anything greater than 4000 through the application UI because this 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.
<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default value</td>
<td>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.</td>
</tr>
<tr>
<td>Display</td>
<td>Indicate whether this field is the display value for reference fields (appears on records that reference this table). Note: This option does not control whether this field is displayed on lists or forms.</td>
</tr>
</tbody>
</table>

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 allow 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 Show Live Feed 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 User role 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 Create access controls 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></td>
</tr>
<tr>
<td></td>
<td>Can be accessed from any application scope.</td>
</tr>
<tr>
<td></td>
<td><strong>This application scope only</strong></td>
</tr>
<tr>
<td></td>
<td>Can be accessed only from the current application scope.</td>
</tr>
<tr>
<td>Can read</td>
<td>Select the check box to allow 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>Can create</td>
<td>Select the check box to allow 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 allow 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 allow 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>
</tbody>
</table>
### Control | Description
---|---
Allow access to this table via web services | Select the check box to allow users to make inbound [Web services](https://www.servicenow.com/) 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.

Allow configuration | Select the check box to allow 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.

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 <strong>unique record identifier</strong> 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>
</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](image)

© 2019 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.
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.

Table Record
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.

Base system tables cannot be deleted. Also, any missing base system tables are recreated when the instance is upgraded. If another table extends to it, you cannot delete a table.

⚠️ Warning: You must delete the records in the table before you delete the table. If you do not delete the records first, errors can result on the parent table if it references the records. Deleting the records removes any references from the parent 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 .
- Minimize triggering an excessive number of business rules as a result of this deletion. Use the setWorkflow(Boolean e) method described at .

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.
Tables & Columns

Click a button to create a new table or application, or browse all applications.

Create Table  Create Application  Browse Applications

Or, select a table to browse its columns and indices.

Table Names
- IBM Mainframe LPAR [cmdb_ci_mainframe_lpar]
- IBM WebSphere [cmdb_ci_app_server_websphere]
- iFrames [content_block_iframe]
- IMAC [change_request_imac]
- Images [db_image]
- Impacted Services [task.cmdb_ci_service]
- Import/Export Map [sys_impex_map]
- Import Log [import_log]
- Import Set [sys_import_set]
- Import Set Row [sys_import_set_row]
- Import Set Row Error [sys_import_set_row_error]
- Inactivity Monitor [sysrule escalate am]
- Inbound Email Actions [sysevent_in_email_action]
- Incident [incident]
- Incident Fact Table [incident_fact_table]
- Incident Metric [incident_metric]
- Incident SLA [incident_sla]
- Incident Time Worked [incident_time_worked]
- Infrastructure Service [cmdb_ci_infra_service]
- Infrastructure Software [cmdb_ci_infra_software]
- Input Parameter [sys_web_service_input]
- Installation Exit [sys_installation_exit]
- Interceptor [sys_wizard]
- Interested Parties [ic_request watcher]
- Internal Workflow Log Entry [wf_log_internal]

Column Names

Column Attributes

Note: Some system tables do not allow this method of deleting records, for example, you cannot delete all user records (sys_user). The list of tables does not include system tables that you cannot delete records from.

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.

<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 ServiceNow Technical 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 are created so that deleted records can be recovered and in-family patch updates, Scripts-Background script executions, and plugin activations for plugins that support rollback contexts can be rolled back.

A rollback context is created when these actions occur.

- A record is deleted using GlideRecord.delete() or GlideRecord.deleteMultiple().
- An in-family upgrade or patch is done.
- A plugin that supports rollback contexts is activated.
- A script is executed using the Scripts-Background module, and the Record for Rollback? item was checked.

The rollback context contains information on all database actions performed by the thread.

Using a rollback context makes it possible to recover from problems caused by a single thread, which means that other database activity is not impacted by the rollback. In the case where another database activity has modified a record that is part of a rollback context, when the rollback context is rolled back, the database field that has been changed is not rolled back.

Because rollback contexts contain significant amounts of data, rollback contexts are deleted after seven days. Deleted records must be restored, and patch upgrades, plugin activations, and background script executions must be rolled back within seven days of the rollback context being created.

To use rollback contexts, the Restore Deleted Records and Delete Recovery plugins must be activated.

Rollback context blacklisted operations

When a rollback context is being created, if these operations are done by the thread, the rollback context is not created, and a roll back is not possible.

- Tables or columns are dropped from the schema. Index drops are okay.
- Re-parenting or promoting a column.
- A table is truncated.
- A table or column is renamed.
- A column type changes.
- A column width is decreased.

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.
- File attachments are not restored when the record is restored.
- 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.

Use the Rollback Contexts module to rollback a patch upgrade or plugin activation

You can use a rollback context to rollback an in-family patch upgrade or a plugin activation for a plugin that supports rollback contexts.

Role required: admin

Rollback contexts are deleted after seven days.

Note: Do not roll back a rollback context until checking with ServiceNow Technical Support. A rollback deletes data and may remove evidence of the upgrade or activation issue preventing debugging of the problem.

1. Navigate to Rollback & Recovery > Recovery Contexts.
2. Click on the rollback context to roll back.
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**.
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, check the **Unique Index** 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.

**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 in certain circumstances. Data lookup rules take precedence over assignment rules.

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. Data lookup and assignment rules run.
3. All ‘before’ business rules that run on a record insert with an order value greater than or equal to 1000.
4. 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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Table</th>
<th>Conditions</th>
<th>Assigned to user, Assigned to group, or Script</th>
</tr>
</thead>
</table>
| Networking | incident| Category is Network      | User: System Administrator  
Group: Network |
<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>Database or Software</td>
<td>Incident</td>
<td>Category is one of Request, Inquiry / Help, Software, Hardware</td>
<td>User: System Administrator&lt;br&gt;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 Item.Category is Request Computers and Hardware</td>
<td>User: System Administrator&lt;br&gt;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>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</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>Note: 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. 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.</td>
</tr>
<tr>
<td>Conditions</td>
<td>The conditions under which the assignment rule applies. In the example, the assignment rule applies when an incident is in the Network category</td>
</tr>
<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>The current.variable_pool set of variables is available.</td>
</tr>
<tr>
<td>Script</td>
<td>A script to specify advanced assignment rule functionality. 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.</td>
</tr>
<tr>
<td>Other fields</td>
<td></td>
</tr>
</tbody>
</table>
### ServiceNow London Now Platform Administration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match conditions</td>
<td>Choices are:</td>
</tr>
<tr>
<td></td>
<td>· Any — If any of the conditions are met, assignment rule applies.</td>
</tr>
<tr>
<td></td>
<td>· All — If all the conditions are met, assignment rule applies.</td>
</tr>
<tr>
<td>Execution Order</td>
<td>The order in which the assignment rule is processed. If assignment rules conflict, a rule with a lower-order value takes precedence over a rule with a higher value. If the order values are set to the same number, the assignment rule with the first matching condition takes precedence over the others. Only the first assignment rule with a matching condition runs against a record.</td>
</tr>
</tbody>
</table>

### Data lookup rules

You can define an assignment rule with Data Lookup and Record Matching Support.

1. Navigate to **System Policy > Rules > Assignment Lookup Rules**.
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>
</tbody>
</table>

© 2019 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>Input value</th>
</tr>
</thead>
<tbody>
<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>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 <strong>incident autoclose</strong> 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 <strong>Activity</strong> field. For more information, see <a href="#">Journal Fields</a>.</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>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>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>Label</td>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------</td>
<td>------------</td>
<td>----------------------------------------------------------------------------------------------</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>Priority</td>
<td>priority</td>
<td>integer</td>
<td>Specifies how high a priority the task should be for the assignee. By default, the <code>calculatePriority</code> business rule calculates this value based on the <code>Impact</code> and <code>Urgency</code> 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 <code>Dictionary overrides</code> 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. For more information on extending tables, see <code>Tables and Classes</code>.</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>Label</td>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------</td>
<td>------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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>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.

#### 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

2019 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.
Modify the task interceptor

You can modify any task interceptor and provide different answers to users.

1. Navigate to **System Definition > Interceptors** (this module may need to be activated).
2. Select the Task Interceptor. The **Answers** related list specifies what choices are presented and where the user is redirected after a choice is selected.
3. Modify the **Answers** related list as desired.
4. After making changes, test the interceptor by clicking **Try It**.

**Note:** To disable the task interceptor, rename it to something other than `task.do`. This renaming disables it without deleting it.
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 Project Portfolio Suite with Financials 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:

![Wizard](https://example.com/wizard.png)

**Planned task**

What type of Planned Task would you like to create?

- Project
- Project Task

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.
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:

The baseline can be viewed on a Gantt Chart using the related link.

**Measure time and effort**

The Planned Task \[\text{planned}\_\text{task}\] table provides standard fields for tracking duration and effort. Duration measures time from start to end date. Effort measures hours of work exerted on the project.

- 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 project amount of work left.
- Percent complete: The Actual effort divided by the Planned effort, which estimates the percentage of planned work which has been completed.

Important planned task table fields
The Planned Task table has these 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>Label</td>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------</td>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</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>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</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>
</tbody>
</table>

### Planned task scripts

Several business rules and one script include power 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>
</tbody>
</table>
### Business Rule and Description

<table>
<thead>
<tr>
<th>Business Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>Auto close milestones</td>
<td>Automatically closes milestones when they are passed.</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.

<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>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.

<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>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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: 15 minutes, 30 minutes, 1 hour, and 2 hours. You can add values to this field as required.</td>
</tr>
<tr>
<td>Note: Internally in the system, the value is always converted to minutes and then stored in the Remind me field.</td>
<td></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.</td>
</tr>
<tr>
<td>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>
<td></td>
</tr>
<tr>
<td>Using</td>
<td>Specifies the method by which the reminder must be sent. Available options are: Send an Email and Outlook Calendar.</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 not to 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 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. Time card users can submit their time cards and time sheets for approval.
- The Time card approvers can approve the time cards in a submitted timesheet by approving the time sheet. Time card approvers can view and approve only those time cards and time sheets that are routed to them for approval. The routing for approval happens 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.
- Time card approvers can use dashboards to view reports of time card and time sheet exceptions, and category wise time reported by the users.
- 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 the project_manager or resource_manager roles.
- The time card admin can create and manage time sheet policies, and can also approve time by exception and process the time sheets. Time card admin can also log time for any users, and edit time cards of any users in Pending or Rejected state.

**Note:** The Time card management plugin is required to use time cards. Some of the procedures on this page require the project management feature, which activates time cards automatically. 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 (com.snc.time_card) plugin. The dashboards for Time Cards must be activated separately using the Performance Analytics - Content Pack - Project Portfolio Suite Dashboards plugin (com.snc.pps_dashboards). You will need a Performance Analytics license to use the dashboards.

**Note:** The Time cards feature also gets activated as part of Project Portfolio Suite with Financials (com.snc.financial_planning_pmo) plugin.

1. Navigate to System Definition > Plugins.
2. Find and click the plugin name.
3. On the System Plugin form, review the plugin details and then click the Activate/Upgrade related link.

   If the plugin depends on other plugins, these plugins are listed along with their activation status.

   If the plugin has optional features that depend on other plugins, those plugins are listed under Some files will not be loaded because these plugins are inactive. The optional features are not installed until the listed plugins are installed (before or after the installation of the current plugin).

4. Optional: If available, 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 practice when you first activate the plugin on a development or test instance.
You can also load demo data after the plugin is activated by clicking the **Load Demo Data** related link on the System Plugin form.

5. Click **Activate**.

---

**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. It is possible to have multiple time sheet policies based on different requirements and workflows in an organization. For example, each department or team may want to specify its own set of time sheet policies, and assign users to them. Time card admin can specify the time sheet policy to which a user belongs.

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 admin, you can create a time sheet policy to specify a different set of policies.

Role required: timecard_admin

1. Navigate to **Time Sheets > Administration > Time Sheet Policies**.
2. Click **New**.
3. 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 policy.</td>
</tr>
<tr>
<td>Allow blank time cards</td>
<td>Allows submitting blank time cards for approval. By default, it is set to false.</td>
</tr>
<tr>
<td>Auto create time card on task update</td>
<td>Auto-creates a user time card when they update a planned task. By default, it is set to false. When a planned task 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 <strong>Assigned to</strong> or <strong>Additional assignee list</strong> field, AND • the task is not in a pending state.</td>
</tr>
</tbody>
</table>

© 2019 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>
</table>
| Auto fill time card with time worked entries      | Auto-fills user time cards with time from their **Time worked** entries. By default, it is set to false. If a time card does not exist for the task, a time card is created when the time worked is updated. The time card is created or updated 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. |
| Auto create time cards every week                 | **Auto-generates time cards** every week through a scheduled job for the users assigned to the time sheet policy. The time cards are generated for a user based on the user’s planned task assignments and hard allocated resource plans.  
  By default, it is set to true.                                                                 |
| Update actual hours and cost in resource plan     | Updates the actual hours and cost in associated resource plan based on the hours entered in the approved time card.  
  If set to true, the system looks for resource plans matching the user and the dates. If a resource plan is found, the resource plan is associated with the time card. The actual hours from the time card entry and the corresponding cost based on the user rate card are then updated in the actual cost field in the resource plan.  
  By default, it is set to false.                                                                 |
| Week starts on                                     | Specifies the start day of the week for the time sheet. The default value is Sunday.                                                                                                                        |
| Maximum hours per day                             | Maximum number of hours a user can fill for any day in a timesheet. The default value is 24.  
  If set to -1, it implies that there is no limit on maximum hours per day. However, the maximum hours entered per day cannot exceed 24 hours. |
| Maximum hours per week                            | Maximum hours a user can fill in a week in a timesheet. The default value is 40.  
  If set to -1, it implies that there is no limit on maximum hours per week.                                                                  |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Non-project time approver | Determines which approvals are required for the non-project tasks.  
  - **Auto**: Time cards are auto-approved when submitted.  
  - **User Manager**: Time cards are routed to the user manager for approval when submitted.  
  - **None**: Users with timecard_admin role can approve time cards.  
  **Note:**  
  - A user manager is one who is selected in the Manager field on User form of the time card user.  
  - A user manager must have time card approver role to view and approve the time cards submitted by a time card user. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Project time approver | Determines which approvals are required for the project tasks.  
  - **Auto**: Time cards are auto-approved when submitted.  
  - **Project Manager**: 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 the user is submitting time.  
  - **User Manager**: Time cards are routed to the user manager for approval when submitted.  
  - **Both**: Time cards are routed to both - user manager, and project manager for approval when submitted.  
  
  **Note**: A time card remains in Submitted state when only either approver approves the time card.  
  - **None**: Time card admin can approve time cards.  
  
  **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, the time card admin can approve time cards. |
| Default Policy        | Indicates if the time sheet policy is a default policy. There can be only one policy with **Default Policy** set to true.  
  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.  
  Any time sheet policy with default policy set to true cannot be deleted. The user must first make another policy as default policy to delete the current default policy. |
**Time sheet policy form related links and lists**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Related links</td>
<td>Sets the current policy as default policy.</td>
</tr>
<tr>
<td>Set as default</td>
<td>Sets the current policy as default policy.</td>
</tr>
<tr>
<td>Related lists</td>
<td>Lists the users who are assigned to the time sheet policy.</td>
</tr>
<tr>
<td>Users</td>
<td>Lists the users who are assigned to the time sheet policy.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.

- **Set** the time sheet policy as default policy, if required.
- **Assign** the time sheet policy to the users.

**Set time sheet policy as default policy**

Time card admin can set a time sheet policy 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.

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 **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** check box on the **record form** is selected to indicate that the current time sheet policy is set as the default policy. Only one time sheet policy can have the **Default Policy** set to true. The **Default Policy** check box on the earlier default time sheet policy is cleared.

Any time sheet policy with **Default Policy** set to true cannot be deleted. The user must first make another policy as default policy to delete the current default policy.

**Assign a time sheet policy to a user**

Time card admin can specify the time sheet policy to which a user belongs.

Role required: timecard_admin

Once a time sheet policy is created, it can be assigned to the required users. Users can be associated to only one time sheet policy.

1. Navigate to **Time Sheets > Administration > Time Sheet Policies**.
2. Open the time sheet policy record.
3. Click **Edit** in the **Users** related list.
4. Use the slushbucket to add the desired users to the policy.
5. Click **Save**.

The selected users appear on the **Users** 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>

**Note:** Inactivating a rate type does not remove it from records where it exists. When time card processing encounters an inactive rate type on the time card, no matching labor rate card is found. In this case, the system rate is used for generating the expense line.

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 a time sheet.
- View notifications for the rejected time cards.

Time Sheet Portal comprises the following sections:

**Header**

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.

Displays the notifications for the rejected time sheets under notifications icon 
. Each entry for the rejected time sheet also displays the number of time cards rejected in the time sheet. Navigate to a rejected time sheet by clicking it in the notification list.
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.

**Group Tasks**

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 a user manager, an option to approve a time sheet is also available.
Logged Time Cards

<table>
<thead>
<tr>
<th>Task</th>
<th>Project time category</th>
<th>Rate type</th>
<th>Sun 15</th>
<th>Mon 16</th>
<th>Tue 17</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task 1</td>
<td>None</td>
<td>Stan...</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Task 1</td>
<td>None</td>
<td>Stan...</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>KTLO</td>
<td>None</td>
<td>Stan...</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Meeting</td>
<td>None</td>
<td>Stan...</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

The Logged Time Cards section displays time cards, in rows, for a given week. Each row provides details such as icon for state of the time card, short description of the task, project time category, rate type, 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](#).

**Note:** The Rate type column is visible only when the Allow multiple rate types check box is selected in the time sheet policy of the user.

A row highlighted in red color indicates a time card in Rejected state. A merge icon in a time card row indicates that a duplicate time card for the same task exists in the time sheet.

When there are no time cards, the Logged Time Cards section displays the Generate Time Cards and Copy from previous time sheet options that you can use 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:** timecard_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 | 1. Click choice list next to Submit.  
2. 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 | 1. Click choice list next to Submit.  
2. 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.

| Create a time card from the Tasks, Group Tasks, or Other tab | 1. On the Tasks, Group Tasks, or Other tab, point to a task (card) that you want to create a time card for.  
2. 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 | 1. On the Tasks tab, select multiple tasks that you want to create time cards for.  
2. Click Add selected to Time Sheet. |
<table>
<thead>
<tr>
<th>Option</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a time card for unassigned task</td>
<td>1. In the Logged Time Cards section, click Add unassigned tasks to Time Sheet.</td>
</tr>
<tr>
<td></td>
<td>2. Enter the task number or short description of the task you worked on during the selected week.</td>
</tr>
</tbody>
</table>

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>
<tbody>
<tr>
<td>Through inline editing</td>
<td>1. Select a row and press Enter. You can also double-click a row.</td>
</tr>
<tr>
<td></td>
<td>2. Edit the values as required.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Through time card form</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Point to a row and click the More Actions icon.</td>
</tr>
<tr>
<td></td>
<td>2. To open the time card form, click Open Form View.</td>
</tr>
<tr>
<td></td>
<td>3. Enter hours on the time card form.</td>
</tr>
<tr>
<td></td>
<td>4. Click Save.</td>
</tr>
</tbody>
</table>

| Add notes to time cards               | 1. Point to a row and click the More Actions icon.                                                                                                                                   |
|                                       | 2. To add a note, click Add Note.                                                                                                                                                      |

Submit time sheet through Time Sheet Portal
Submit a time sheet for a given week.

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 when 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. A user manager is one who is selected in the Manager field on User form of the time card user.
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 log time 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 button appears in the Time Sheet section. The Approve button appears only for a user manager.

Once you have submitted the time sheet for your resource, you can click Approve to approve it. Only the time cards that are routed to the user manager, are approved. 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.

A time sheet can have any of the following states:

- Pending
- Submitted
- Approved
- Processed
- Rejected

**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.
### Option Steps

**From the time sheet menu**

Navigate to Time Sheets > My Time Sheets > Current (This Week).

The time sheet form for the current week opens.

**From the time sheet list**

1. Navigate to Time Sheets > My Time Sheets > All > New.
2. Click New.

### 2. On the form, fill in the fields.

#### Time Sheet form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Note:</th>
<th>time sheet policy Week starts on controls the start day of the week.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Week starts on</td>
<td>Starting date of the week for which the time sheet is created.</td>
<td></td>
<td></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 associated time cards.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>Name of the user for which time sheet is created.</td>
<td></td>
<td></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>
<td></td>
<td></td>
</tr>
<tr>
<td>Comments</td>
<td>Comments related to the time sheet.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notes</td>
<td>Any additional information.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 3. Click Submit.

Add time cards to the time sheet. You can use the following related links and related list to add time cards. You can also add time cards using the Time Sheet Portal.

#### Time sheet form related links and lists

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Related links</td>
<td></td>
</tr>
<tr>
<td>Generate Time Cards</td>
<td>Link to generate time cards for the assigned project tasks.</td>
</tr>
<tr>
<td>Copy from previous time sheet</td>
<td>Link to open the Copy Time Sheet window for you to copy the time cards from previous time sheets.</td>
</tr>
</tbody>
</table>
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. A user manager is one who is selected in the Manager field on User form of the time card user.

Role required: timecard_approver or timecard_admin

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 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.

Time cards for the project tasks can be associated with relevant *resource plans*.

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
- Rejected

**Create a time card**

Time cards can be created automatically or manually.

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.

- 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 *time sheet policy* **Auto create time card on task update** 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 added to 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.

  **Note:** Time cards cannot be created automatically when you use the mobile interface. Use the desktop interface if you want to use the automatic time card feature.

- Manual: Create a time card for each task and enter the time manually.

1. Create the time card with one of these options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Steps</th>
</tr>
</thead>
</table>
   | **From a time sheet related list** | 1. Open the time sheet that you want to create the time card for.  
   |                                | 2. Click **New** in the **Time Cards** related list.                |
   | **From a time sheet related link** | 1. Open the time sheet where you want to create the time card.  
   |                                | 2. Click any of the following related links. These options are also available on the **time sheet portal**: |
   |                                | - **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.

   | From time sheet portal | 1. Navigate to **Time Sheets > Time Sheet Portal**. |

© 2019 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.
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 that the time sheet is created for. The field is automatically filled.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The time sheet policy Week starts on controls the start day of the week.</td>
</tr>
<tr>
<td>State</td>
<td>Current state of the time card. All new time cards begin in the Pending state. Default states: Pending, Submitted, Approved, Processed, and Rejected.</td>
</tr>
<tr>
<td>Category</td>
<td>Type of task that the time card is created for.</td>
</tr>
<tr>
<td>Task</td>
<td>Task that the time card is associated to.</td>
</tr>
<tr>
<td>Project time category</td>
<td>Type of activity in the project that time is reported for. The field is available only when Category is set to Project/Project Task.</td>
</tr>
<tr>
<td>User</td>
<td>Name of the user that the time card is created for.</td>
</tr>
<tr>
<td>Rate type</td>
<td>Rate type that is considered during the expense line generation. See Rate type in labor rate card for more information.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This field is visible only when the Allow multiple rate types check box 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></td>
<td><strong>Note:</strong> 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.

Note:

- 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 time sheets 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. 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.

**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.

**Note:** If a time sheet is rejected, it gets listed in the notifications for the rejected time sheets under notifications icon on Time Sheet Portal.

- If Project time approver is set to Both in the time sheet policy assigned to the user, the time card remains in Submitted state only when either approver approves the time card. If one of the approver rejects, the time card state is set to the Rejected, and the Approved by field is cleared, requiring approval of both approvers on resubmission.

### 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 started](image)

**Time counter stopped:**

![Time worked stopped](image)

If you are creating time cards from time worked entries, you can add the 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.

![Time Card](image)

**Time worked notice**

**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.
Enable the cost management feature. When a time card is marked Approved, the user's rate (listed in the Labor Rate Card) is used to generate a one-time Expense Line for the time worked. If no Labor Rate Cards apply to the user, the property `com.snc.time_card.default_rate` defines a default rate.

**Roles**

The timecard_admin role enables users to approve, modify, and delete the time cards of other users.

**Domain separation in Time Card**

This is an overview of domain separation in Time Card. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can then control several aspects of this separation, including which users can see and access data.

**Overview**

**Support: Data only**

Domain separation in this application is supported at the Data only level, meaning it supports the data security model of separating visibility of data from one domain to another. 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

As the process takes place, it updates any field designated as a workflow field.

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.

- Planned Task
- Field Service Management
- Project Management
- Governance, Risk, and Compliance

*Note: Contact ServiceNow to activate the plugin by itself.*

1. In the HI Service Portal, click **Service Requests > Activate Plugin**.
2. Fill out the form.

<table>
<thead>
<tr>
<th>Target Instance</th>
<th>Instance on which to activate the plugin.</th>
</tr>
</thead>
<tbody>
<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>Date and time must be at least 2 business days from the current time.</td>
</tr>
<tr>
<td>Reason/Comments</td>
<td>Provide any information that would be helpful for the ServiceNow personnel activating the plugin. For example, if you need the plugin activated at a specific time instead of during one of the default activation windows.</td>
</tr>
</tbody>
</table>

3. 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.
UI Actions examples

Below are a few examples.

**Warning:** These examples may not work on all instances. They are provided as illustrative 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");
```
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.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.
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.
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.
Field Labels

System dictionary

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.
- 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>
</tbody>
</table>

**Note:** The list shows only tables and database views that are in the same scope as the dictionary override.

<p>| Override reference qualifier | Select the check box to display the Reference qualifier field, which overrides the reference qualifier for the field on the extended table. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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></td>
<td><strong>Note:</strong> 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. 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>
</table>
| Table        | Defines the table in which the element is created.  
  
  **Note:** This list shows only the tables that meet the scope protections for adding fields. |
| Type         | Defines the field type of the column or, if the *Type* is *Collection*, 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. |
| Active       | Enables or disables the field. When this check box is cleared, the field is not used by the system.                                           |
| Function field| 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. |
| Read only    | 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.  
  
  **Note:** You can override this option for extended tables. |
| Audit        | Enables or disables auditing for a table. Turning on Auditing (History) for a Table.  
  
  **Note:** This option only applies to tables. |
| Text index   | Determines whether searches index the text in a table.  
  
  **Note:** This option only applies to tables. To exclude fields from indexing, see *Remove an Index for a Specific Field*. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Column label     | Defines a unique label for the column. The label appears on list headers and form fields for the column.  
   - Updating the **Column label** 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 u_ to indicate that it is custom. For example, if you enter **Activity Description** as the column label, the column name defaults to **u_activity_description**. |
| Column name      | 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:  
   - 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.  
   - 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.  
   - For a field in a global application, the name is prefixed with u_ to indicate that it is custom.  
   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. |
<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>Mandatory</td>
<td>Determines whether this field must contain a value to save a record. For more information, see Creating Mandatory Fields.</td>
</tr>
</tbody>
</table>

**Note:**
- You can only change this value for a **String** field. Changes for any other type of field are ignored.
- 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.
- 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.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Display            | 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 **Number** field is the display value for all task tables. **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](#). |
| Function definition| Defines the function that the field performs.  
  Starts with `glidefunction:`, followed by the operation to be performed (for example, `concat`), 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:  
  
  ```
  glidefunction:concat(short_description, ' ', caller_id.name)
  ```
  **Note:** Function parameters support dot walking. See [Selecting fields on related tables using dot-walking](#). |
<p>| Attributes (Advanced view) | Alters the behavior of a field or functionality that depends on the field. For more information, see <a href="#">Dictionary Attributes</a>. Attributes can be overridden for extended tables with <a href="#">dictionary overrides</a>. You can also configure attributes for this dictionary entry through the Attributes related list. |
| Default Value      | Use dynamic default (Advanced view) | Allows you to specify a default value that is generated dynamically based on a dynamic filter. |
|                    | Dynamic filter value (Advanced view) | Specifies the dynamic filter that determines the default value if the Use dynamic default option is selected. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td>Reference Specification</td>
<td></td>
</tr>
<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>
<tr>
<td>Use reference qualifier (Advanced view)</td>
<td>Specifies the type of qualifier to use:</td>
</tr>
<tr>
<td></td>
<td>- Simple: A set of choice lists where you can specify a reference qualifier condition.</td>
</tr>
<tr>
<td></td>
<td>- Dynamic: A dynamic filter that you can use to build the qualifier.</td>
</tr>
<tr>
<td></td>
<td>- Advanced: A static encoded query string or JavaScript code that you can use to build the qualifier.</td>
</tr>
<tr>
<td>Reference qual condition</td>
<td>Specifies a condition when the reference qualifier runs if the Simple qualifier type is selected.</td>
</tr>
<tr>
<td>Dynamic ref qual (Advanced view)</td>
<td>Specifies the dynamic filter that determines the reference qualifier when the Dynamic qualifier type is selected.</td>
</tr>
<tr>
<td>Reference qual (Advanced view)</td>
<td>Filters the records available for a reference field if the Advanced qualifier type is selected. Reference qualifiers can be overridden with dictionary overrides.</td>
</tr>
<tr>
<td>Reference key (Advanced view)</td>
<td>Identifies a field other than sys_id to use as the unique identifier for reference fields.</td>
</tr>
<tr>
<td>Reference cascade rule (Advanced view)</td>
<td>Defines what happens to a record if the record it references is deleted. Select one of the following options:</td>
</tr>
<tr>
<td></td>
<td>- Clear: Clears the references (default).</td>
</tr>
<tr>
<td></td>
<td>- Delete: Deletes all referencing records.</td>
</tr>
<tr>
<td></td>
<td>- Restrict: Prevents record deletion if there is a referencing record.</td>
</tr>
<tr>
<td></td>
<td>- None: Does not change referencing records.</td>
</tr>
<tr>
<td>Reference floats (Advanced view)</td>
<td>Enables the Edit button on related lists for one-to-many relationships.</td>
</tr>
<tr>
<td>Dynamic creation (Advanced view)</td>
<td>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.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Dynamic creation script (Advanced view)</td>
<td>When the <strong>Dynamic creation field</strong> is selected, allows you to enter a script for creating a record on the referenced table.</td>
</tr>
<tr>
<td>Dependent Field</td>
<td></td>
</tr>
<tr>
<td>Dependent on field (Advanced view)</td>
<td>Specifies a field on which the current field depends. For more information, see <a href="#">Configuring Dependent Fields</a>. Note: You can override this value for extended tables.</td>
</tr>
<tr>
<td>Choice List Specification</td>
<td></td>
</tr>
<tr>
<td>Choice</td>
<td>Allows users to see a list of suggested values in one of the following ways:</td>
</tr>
<tr>
<td></td>
<td>· List menu without -- None --</td>
</tr>
<tr>
<td></td>
<td>· List menu with -- None --</td>
</tr>
<tr>
<td></td>
<td>· Suggestion</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Choice table (Advanced view)</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Choice field (Advanced view)</td>
<td>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.</td>
</tr>
<tr>
<td>Calculated Value</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Calculated (Advanced view)</td>
<td>Determines whether the value of the field is calculated from other values. If selected, use the <strong>Calculation</strong> 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.</td>
</tr>
<tr>
<td>Note:</td>
<td>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.</td>
</tr>
</tbody>
</table>
| Calculation (Advanced view)| When the **Calculated** field is selected, allows you to enter a script for calculating the value of the field. These can be overridden for extended tables with dictionary overrides. You can use the current object in this script. As with access control rules, the script can:  
  • Evaluate to true or false.  
  • Return an answer variable set to true or false.  
  • Set a field value directly, such as:  
    current.display_name="name". |

**Additional fields**

<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 <strong>Tables and Classes</strong>.</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 <strong>Adding Spell Check to a Field</strong>.</td>
</tr>
<tr>
<td>Unique</td>
<td>Requires the field value to be unique.</td>
</tr>
<tr>
<td></td>
<td><strong>Warning:</strong> Making a field unique when the corresponding table already has different values for that field causes data loss. Before you enforce uniqueness on a field, verify that no records in the table for the field have values, or that they all have the same value.</td>
</tr>
</tbody>
</table>

UI action
### 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 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, allows entering &quot;None&quot; as the 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>allow_public</td>
<td>true/false</td>
<td>table_name field</td>
<td>If true, the table name field will display 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>approval_user</td>
<td>name of field containing the user(s) for the approval type this field represents</td>
<td>integer field</td>
<td>The fields of the table are used to perform the lookup using a matcher. Approvals are specified as fields in the table that have an attribute of approval_user=&lt;field_name&gt;, where &lt;field_name&gt; 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.</td>
</tr>
<tr>
<td>attachment_index</td>
<td>true/false</td>
<td>any table</td>
<td>If true, attachments on the table are indexed for search purposes. See <a href="#">index attachments on a table</a>.</td>
</tr>
<tr>
<td>barcode</td>
<td>true/false</td>
<td>string field</td>
<td>Allows a string field in the <a href="#">Using the ServiceNow Classic mobile app</a> to access a camera on a mobile device to scan and process a bar code.</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>base_table</td>
<td>name of base table type</td>
<td>table_name field</td>
<td>A table_name field allows the user to choose any table derived from the table specified by this attribute. By default, the base table itself is also included in the choice list (but see skip_root to turn off this behavior).</td>
</tr>
<tr>
<td>calendar_elements</td>
<td>list of field names, separated by semicolons (;)</td>
<td>any calendar event table</td>
<td>Specifies a list of fields to be used when constructing the description of a calendar event. If not specified, the usual display name plus short description are used. The calendar_elements 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 '01:02:30' for one hour, two minutes, and thirty 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 — identifies 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 allows tracking the entry of critical information.</td>
</tr>
<tr>
<td>current_location</td>
<td>true/false</td>
<td>string field</td>
<td>Allows 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 Execute Now button. This attribute is used by applications using schedules (such as Discovery) to substitute their own more appropriate action.</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>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 — identifies 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 — identifies the default working state value for a task table.</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 <strong>detail_row</strong> for each record in the list view. UI15 is required to use this attribute.</td>
</tr>
</tbody>
</table>
| document_viewer_audit | view, download, or all         | any table        | When the Document Viewer is enabled, this attribute keeps a record of user actions performed on attachments. The values are:  
  - **view**: enables an audit when users view an attachment  
  - **download**: supplies audit information for only downloaded attachments  
  - **all**: shows audit information when attachments are viewed and downloaded |
<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
<th>Target Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 clicked, a popup 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>field_list_selector</td>
<td>true/false</td>
<td>any glide_list</td>
<td>Allows the user to select a field from the dependent table (or current if dependent is not specified). This attribute is used in some workflow activities.</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>
<tr>
<td>format</td>
<td>format name</td>
<td>any numeric field</td>
<td>Specifies a named format to use instead of the standard numeric formatting. Options are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• glide_duration: Formats a time specified in milliseconds as <em>ddd hh:mm:ss</em>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• none: Disables automatic number formatting (for example, changes 2,500 to 2500).</td>
</tr>
<tr>
<td>glide.db.oracle.ps.query</td>
<td>true/false</td>
<td>any table</td>
<td>If present and false, prevents the use of Oracle prepared queries on the 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>global_visibility</td>
<td>true/false</td>
<td>any table with a sys_domain column</td>
<td>If present or true, makes this table visible globally even if there are domain restrictions (that is, the sys_domain field has a value).</td>
</tr>
<tr>
<td>hasLabels</td>
<td>true/false</td>
<td>any table</td>
<td>If present or true, marks this table as being the target of a label at some point. This attribute can be set manually, but it is set automatically whenever a label is generated. When true, the label engine runs on any change to the table, updating the labels as needed.</td>
</tr>
<tr>
<td>hasListeners</td>
<td>true/false</td>
<td>any table</td>
<td>If present or true, marks this table as available for listeners to get events (insert, update, delete) on.</td>
</tr>
<tr>
<td>hasWorkflow</td>
<td>true/false</td>
<td>any table</td>
<td>Tells 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, HTML sanitization is enabled for the selected HTML or Translated HTML field. By default, HTML Sanitization is performed 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, sanitization is performed 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>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>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 be used when the table is used in a module or BSM map. 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. Overriden by the ORDERBY URL parameter or 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 be executed iteratively. Otherwise, some deletes may be performed using a more efficient bulk method.</td>
</tr>
<tr>
<td>json_view</td>
<td>true/false</td>
<td>any table</td>
<td>Enables an icon next to a field that, when clicked, displays data interchange information if a JSON object is associated with the field.</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 (see knowledge_custom).</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>largeTable</td>
<td>true/false</td>
<td>any table</td>
<td>If present or true, marks this table as 'large' 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, causes a call to a JavaScript function named &lt;tableName&gt;_&lt;fieldName&gt;Listen or globalListen if that function does not exist. The function is called with arguments (tableName, fieldName, oldValue, newValue).</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 the choice between the Live Feed for that record (also known as a document feed) or the activity formatter fields already in use. See Activity formatter for more details.</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>long_label</td>
<td>true/false</td>
<td>any reference field</td>
<td>Long or short labels refer to the label displayed 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 just be Email. Usually the placement of the reference field on the form makes it clear what the field represents. The global property (<code>glide.short.labels</code>) is used to specify the type of labels displayed for all reference fields on any form. This global property can be overridden 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>maintain_order</td>
<td>true/false</td>
<td>any glide_list</td>
<td>If present or true, displays the up/down arrow order buttons to the right of the list of selected items.</td>
</tr>
<tr>
<td>mode_toggler</td>
<td>true/false</td>
<td>any composite_name field</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>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>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, the model for the workflow activity is built 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>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_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>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_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 a record from this table is deleted. 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. This attribute is 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 Watch list field.</td>
</tr>
<tr>
<td>no_multiple</td>
<td>true/false</td>
<td>any glide_list field</td>
<td>Hides the select multiple icon.</td>
</tr>
<tr>
<td>no_optimize</td>
<td>true/false</td>
<td>any table affected by the table cleaner.</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.</td>
</tr>
<tr>
<td>no_text_index</td>
<td>true/false</td>
<td>any field on a text indexed table</td>
<td>If a table is text indexed, the no_text_index attribute on a field prevents this field from being included in the text index.</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_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 <strong>Number of characters displayed in list cells</strong> which is 40 by default.</td>
</tr>
<tr>
<td>no_update</td>
<td>true/false</td>
<td>table</td>
<td>Is 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 it is created. Does not stop the table from being updated. This attribute 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>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. Online schema changes provides 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. 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>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>order</td>
<td>numeric value</td>
<td>model variable fields</td>
<td>Used internally only (for model variables).</td>
</tr>
<tr>
<td>popup_processor</td>
<td>binary Java class name</td>
<td>any field or table</td>
<td>Specifies a custom popup 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 the conditions field to be rendered 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 semicolons</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. See the cmdb_ci field (Configuration Item) on the Incident form for a working example.</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 ref_ac_columns attribute. This attribute overrides the default behavior, which searches only the display value column. See <a href="#">Configure auto-complete to match text from any reference field</a>.</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 auto-complete only matches text from 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. See <a href="#">Remove the display value column</a>.</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>
</tbody>
</table>

© 2019 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>Name</th>
<th>Value</th>
<th>Target Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ref_autoCompleter</td>
<td>JavaScript class name</td>
<td>any reference field (can be applied to a table to affect all reference fields on the table.)</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>- <strong>AJAXReferenceCompleter:</strong> Displays matching auto-complete choices as a choice-list. The list only displays the display value column of the reference table. 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>- <strong>AJAXTableCompleter:</strong> Displays matching auto-complete choices as rows in a table. The table displays the display value column of the reference table and any columns listed in the <code>ref_ac_columns</code> attribute.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- <strong>AJAXReferenceChoice:</strong> Displays matching auto-complete choices as a choice-list. The list only displays the display value column of the reference table. 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.</td>
</tr>
</tbody>
</table>

For more information, see [Auto-complete for reference fields](#).
<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
<th>Target Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ref_contributions</td>
<td>UI Macro name list, separated by semicolons (&quot;;&quot;)</td>
<td>any reference field</td>
<td>Causes the named UI macro to be invoked when the field is rendered on a form.</td>
</tr>
<tr>
<td>ref_decoration_disabled</td>
<td>true/false</td>
<td>any reference field</td>
<td>When set to true, disables display of the reference icon on a selected field.</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 be sent 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 that should be used to order the choice 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 are displayed 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>restrictTo</td>
<td>field name (including indirect, dot-walked field references)</td>
<td>any conditions field</td>
<td>Specifies the field that contains the comma-separated list of fields that the conditions should be restricted to using.</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 label of the field, 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 the Decimal field type. The default is 2. This attribute is applied to the Max Length of the field. <strong>Note:</strong> Increase the Max Length to a value greater than 15 to increase this attribute.</td>
</tr>
<tr>
<td>script</td>
<td>a function that returns the contents of the field</td>
<td>any slushbucket field</td>
<td>Allows you to write a script to define what is loaded into the slushbucket field.</td>
</tr>
<tr>
<td>short_label</td>
<td>true/false</td>
<td>any reference field</td>
<td>Long or short labels refer to the label displayed for reference fields on a form. For example, if the field contains the caller’s email address, the long label would be Caller Email, while the short label would just be Email. Usually the placement of the field on the form makes it clear what the field represents. The global property (glide.short.labels) is used to specify the type of labels displayed for all reference fields on any form. This global property can be overridden for any reference field by setting the short_label=true or long_label=true 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>Allows users to select documents from system tables. For example, sys_script or sys_user. By default, users cannot select records from system tables.</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>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 would be returned by a set of conditions. 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 choice list (see base_table for more details).</td>
</tr>
<tr>
<td>sla_basis</td>
<td>list of table names separated by semicolons (';')</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>sla_closure</td>
<td>list of table names separated by semicolons (';')</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>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 slushbucket.</td>
</tr>
<tr>
<td>smallTable</td>
<td>true/false</td>
<td>any table</td>
<td>If present or true, marks this table as &quot;small&quot; (that is, not large) for the purposes of our querying strategy. Without this attribute or the largeTable attribute, the glide.db.large.threshold property, or the 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>Defines 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. Most likely useful on HTML fields.</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>synch_attachments</td>
<td>true/false</td>
<td>any table</td>
<td>Similar to <strong>update_synch</strong> but writes the file attachments of the record to update sets. See <a href="#">index attachments on a table</a>.</td>
</tr>
<tr>
<td>table</td>
<td>name of table</td>
<td>field_name field</td>
<td>Displays the fields of the table specified.</td>
</tr>
<tr>
<td>tableChoicesScript</td>
<td>name of script include</td>
<td>table_name field</td>
<td>The name of a script include whose <code>process()</code> 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 popup on a reference field.</td>
</tr>
<tr>
<td>text_index_filter_junk</td>
<td>true/false</td>
<td>any table</td>
<td>Set the value to <code>false</code> to <strong>disable the junk filter</strong> for the 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>
</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>
</tbody>
</table>

© 2019 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>Name</th>
<th>Value</th>
<th>Target Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>time_zone_field</td>
<td>name of field containing the timezone</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>
</tbody>
</table>
| timeDimension    | true/false                  | any field of date type (glide_date_time, glide_date, due_date, date, or datetime) in a table subclassed from the task table | 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).
|                  |                             |                         | **Note:** OLAP functionality has been deprecated.                            |
| tree_picker      | true/false                  | reference field with reference to a hierarchical table | Displays the hierarchy of reference values in a tree display (such as locations). |
| ts_weight        | integer value               | any field               | Controls the relative importance of a match in the field for text search. See [Control Match Relevance By Field](#). |
| types            | list of valid element types separated by semicolons (`,`) | field_name field        | Limits the fields display to the specified types.                           |
| update_synch     | true/false                  | any table               | 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](#). |
| use_document_viewer | true/false              | any table               | If present or true, allows users to open supported attachments in a document viewer within the platform, rather than downloading the files directly to their own file system. |
| use_workflow     | true/false                  | any table that has delivery plans or uses workflow | If present or true, causes workflow to be used instead of delivery plans. |
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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
<th>Target Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
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.

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.

You can revert this functionality to legacy behavior and require explicit read ACLs to be added to
the database views. Set the glide.security.expander.view.legacy property to true. For upgraded
instances, add this property to the system, and set it to true for the same legacy behavior in pre-
Istanbul releases, or set to false to use the new behavior.
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 names the table to join to the database view. Assign a Variable prefix to use when 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.
The **Where clause** supports these JavaScript conditional operators:
1. From the Database View form, click **New** on the View Tables related list.
2. **Configuring the form layout** 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 for 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 shows a value of **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
   ```
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 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 10,000. 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 not present to support the view, the form looks like this:
Database View

pm_project sla

Name: pm_project sla

Description: Join pm_project to sla(task_sla) to report on things like project names by sla.

Related Links
Try It

View Tables

View = pm_project sla

Table: task_sla
Order: 100
Variable prefix: taskslatable

Table: pm_project
Order: 100
Variable prefix: pmp

Actions on selected rows...

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.

<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 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 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>Name</td>
<td>Description</td>
<td>Label</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------</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>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>
</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 Configure &gt; List Layout.</td>
</tr>
<tr>
<td>List v3</td>
<td>Open the list title menu and select List Layout.</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 case, 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.

![List v2 list calculation window](image)

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.

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.

<table>
<thead>
<tr>
<th>List Control form</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
</tr>
<tr>
<td>Table</td>
</tr>
<tr>
<td>Related list</td>
</tr>
<tr>
<td>Label</td>
</tr>
<tr>
<td>Omit new button</td>
</tr>
<tr>
<td>Omit edit button</td>
</tr>
<tr>
<td>Omit if empty</td>
</tr>
<tr>
<td>Omit columns if empty</td>
</tr>
<tr>
<td>Field</td>
</tr>
<tr>
<td>-----------------------</td>
</tr>
<tr>
<td>Omit filters</td>
</tr>
<tr>
<td>Omit links</td>
</tr>
<tr>
<td>Omit drill-down link</td>
</tr>
</tbody>
</table>
| List edit type        | Controls the ability of a user to edit values directly in individual cells in a list. The options are:  
  - Save immediately (cell edit mode): enables cell editing. The entire row is saved when the user enters a new value.  
  - Save data by rows: enables cell editing. The row is saved only when the user navigates away from the row or clicks the Save icon (✔). This mode allows the user to modify multiple values before saving a record.  
  - Disable list editing: prevents users from editing cells in the list.  
This field is available for standard lists only.                                                                                                                                                                                                                                                                 |
<p>| List edit tag         | Enter an arbitrary string of letters or numbers to create a unique tag that is sent to a reference qualifier as the script variable listEditRefQualTag.                                                                                                                                                                                                                                                                                        |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>List edit insert row</td>
<td>Select the check box to enable or clear the check box to disable the ability for a user to create records in list view. When it is enabled, an empty row appears at the bottom of the list. This field is available for standard lists only.</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>Hierarchical lists</td>
<td>Inserts a <strong>hierarchical list</strong> 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>
<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>Edit default filter</td>
<td>Specify the filter to apply by default when this list is opened. The edit default filter control is specific to related lists. The option does not appear for standard lists.</td>
</tr>
<tr>
<td>New roles</td>
<td>Specify the 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>Edit roles</td>
<td>Specify the user roles required to have the <strong>Edit</strong> button appear in the list. This field is available for standard lists only.</td>
</tr>
<tr>
<td>Filter roles</td>
<td>Specify the 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>Specify the user roles required to have links generated for fields that reference other files. This field is available for standard lists only.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Disable list v3</td>
<td>Select the check box to disable List v3 for this list. For more information, see <a href="#">Disable List v3 for a specific list</a>. This field is available for standard lists only, when List v3 is activated.</td>
</tr>
<tr>
<td>Default view mode</td>
<td>Choose whether to load this list in List v3 <a href="#">Grid</a> or <a href="#">Split</a> mode by default. For more information, see <a href="#">List v3 split mode</a>. This field is available for standard lists only, when List v3 is activated.</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. Click 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) {
```
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 in 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:** The `isOrder` attribute can define which field is used for list sorting, but it 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.

```plaintext
Arguments:
&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:

```plaintext
&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:

```plaintext
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 `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 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>

3. On the List Control form, select the desired settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>List edit type</td>
<td>Controls the ability of a user to edit values directly in individual cells in a list. The options are:</td>
</tr>
<tr>
<td></td>
<td>• Save immediately (cell edit mode): enables cell editing. The entire row is saved when the user enters a new value.</td>
</tr>
<tr>
<td></td>
<td>• Save data by rows: enables cell editing. The row is saved only when the user navigates away from the row or clicks the Save icon (✔️). This mode allows the user to modify multiple values before saving a record.</td>
</tr>
<tr>
<td></td>
<td>• Disable list editing: prevents users from editing cells in the list.</td>
</tr>
<tr>
<td></td>
<td>This field is available for standard lists only.</td>
</tr>
</tbody>
</table>
### Field: List edit insert row

Select the check box to enable or clear the check box to disable the ability for a user to create records in list view. When it is enabled, an empty row appears at the bottom of the list.

This field is available for standard lists only.

**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 insert row</td>
<td>Select the check box to enable or clear the check box to disable the 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>

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>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.ui.list.detail_row</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:

| UI16       | Point to the application menu that contains the module to edit and click the edit application (pencil) icon. |
To open the module directly, point to the module and click the edit module (pencil) icon.

| UI15 | Right-click the application in the navigation pane and select Edit Application. |

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 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>

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() {
  }
};
```
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`. If it does not exist, click New.
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><code>glide.ui.breadcrumb_max_entries</code></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 (½).

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

For evaluation, you can activate the plugin for an application that requires a purchased subscription on a non-production instance. To activate the plugin on production instances, you must purchase the subscription. To purchase a subscription, contact your ServiceNow account manager. For details on purchasing a plugin, see Purchase a plugin.

Some plugins require activation by ServiceNow personnel. Request these plugins through the HI Customer Service System instead of activating them yourself. For details, see Request a plugin.

For plugins that you can activate yourself, continue with the following steps.

1. Navigate to **System Definition > Plugins**.
2. Find and click the plugin name.

3. On the System Plugin form, review the plugin details and then click the **Activate/Upgrade** related link.

   If the plugin depends on other plugins, these plugins are listed along with their activation status.

   If the plugin has optional features that depend on other plugins, those plugins are listed under **Some files will not be loaded because these plugins are inactive**. The optional features are not installed until the listed plugins are installed (before or after the installation of the current plugin).

4. Optional: If available, 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 practice when you first activate the plugin on a development or test instance.

   You can also load demo data after the plugin is activated by clicking the **Load Demo Data Only** related link on the System Plugin form.

5. Click **Activate**.

---

**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**.
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.
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. Note: The list shows only tables and database views that are in the same scope as the context menu.</td>
</tr>
</tbody>
</table>
| Menu      | Select the list context menu in which this option appears.  
  - List title menus  
  - Column headings  
  - List row menu                                                                                                                                                                                                                                                                                        |
| Type      | Select the type of menu option to create:  
  - **Action**: A menu option that performs an immediate action.  
  - **Menu**: Creates a parent menu that can display a submenu.  
  - **Separator**: 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.  
  - **Label**: Create an unlinked label for a menu or section of a menu.  
  - **Dynamic actions**: Menu options dynamically created, such as the available views or user filters that can only be generated at the time the list is displayed.                                                                                                                                                         |
<p>| Name      | Enter the label for the action as it will appear in the menu.                                                                                                                                                                                                                                                                                                      |
| Parent    | 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.                                                                                                                                                                                                                             |
| Order     | Assign an order number to this item, menu, or separator to specify where in the menu it appears.                                                                                                                                                                                                                                                                  |
| Active    | Enable or disable this context menu item. Only active items are shown in the context menu.                                                                                                                                                                                                                                                                       |
| Run onShow script | Select this check box to display the onShow script field.                                                                                                                                                                                                                                                                                                       |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 <a href="#">Action script for List v2 context menus</a>.</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 <a href="#">Dynamic actions script for List v2 context menus</a>.</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 <a href="#">onShow script for List v2 context menus</a>.</td>
</tr>
</tbody>
</table>
```javascript
// This server-side script is used to dynamically create actions for the context menu, such as the list of available templates.
// Add items to the context menu by calling:
// g_contextMenu.addActions(item_id, label, script_string, order);
//
function buildContextActions() {
  var queryGen = new GlideCollectionQueryCalculator();
  var query = queryGen.buildQueryClause(g_tableName, 'name');
  g_contextMenu.addAction('dictionary', g_itemName, "showDatabaseView" + query + "'", g_itemOrder);
}
```
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:

#### onShow script variables

<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 web browser notes**

**Important:** Due to significant performance issues, ServiceNow recommends that customers utilize a modern browser for its products and 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 Security Mode to High (via 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 (x), 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>
<tbody>
<tr>
<td><code>glide.ui.admin_import_xml_roles</code></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>- Type: string</td>
</tr>
<tr>
<td></td>
<td>- Default value: admin</td>
</tr>
<tr>
<td></td>
<td>- Location: System Property (sys_properties) table</td>
</tr>
<tr>
<td>Property</td>
<td>Usage</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
</tbody>
</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 |
| glide.ui.list_v3.append_module_title        | 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 Incident > All, the list title is Incidents (All).  
  - Type: true | false  
  - Default value: true  
  - Location: System Property (sys_properties) table |
| glide.ui.list_v3.chart_limit                | Sets the maximum number of groups to display in list grouping charts.  
  - Type: integer  
  - Default value: 12  
  - Location: Add to the System Property (sys_properties) table |
| glide.ui.list_v3.debug_compatibility.roles  | 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.  
  - Type: string  
  - Default value: admin  
  - Location: Add to the System Property (sys_properties) table |
| Enable List v3                               | Determines whether List v3 is enabled globally. Additional conditions may prevent incompatible lists from loading in List v3, even when this property is enabled.  
  - Type: true | false  
  - Default value: true  
  - Location: System Properties > List v3  
  - Learn more: Disable List v3 globally |
| glide.ui.list_v3.limit_chart_data           | Determines whether list grouping charts display the Other category when the number of groups exceeds the value set in the glide.ui.list_v3.chart_limit property.  
  - Type: true | false  
  - Default value: true  
  - Location: Add to the System Property (sys_properties) table |
<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable List v3 for Related Lists on Forms</td>
<td>Determines whether List v3 is enabled for related lists. The <code>glide.ui.list_v3.enable</code> property must be set to <code>true</code> to enable List v3 for related lists.</td>
</tr>
<tr>
<td><code>glide.ui.list_v3.related_list</code></td>
<td>- Type: choice list</td>
</tr>
<tr>
<td></td>
<td>- Default value: <code>enable_async_v2</code></td>
</tr>
<tr>
<td></td>
<td>- Available values:</td>
</tr>
<tr>
<td></td>
<td>- <code>off</code>: Disables List v3 for related lists. List v2 is used.</td>
</tr>
<tr>
<td></td>
<td>- <code>enable_v3</code>: Enables List v3 for related lists.</td>
</tr>
<tr>
<td></td>
<td>- <code>enable_async_v2</code>: Uses list v2 for related lists, but loads them asynchronously. When form tabs are enabled, only the lists on the visible tab are loaded.</td>
</tr>
<tr>
<td></td>
<td>- Location: <code>System Properties &gt; List v3</code></td>
</tr>
<tr>
<td></td>
<td>- Learn more: <a href="#">Enable List v3 for related lists</a></td>
</tr>
<tr>
<td>Enables real-time record updates on List v3 (Note: this may impact system performance)</td>
<td>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.</td>
</tr>
<tr>
<td><code>glide.ui16.live_lists.enabled</code></td>
<td>- Type: <code>true</code></td>
</tr>
<tr>
<td></td>
<td>- Default value: <code>true</code></td>
</tr>
<tr>
<td></td>
<td>- Location: <code>System Properties &gt; List v3</code></td>
</tr>
<tr>
<td>Allow related list query conditions to be added through the filter</td>
<td>Determines whether the related list conditions builder is enabled for List v3 list views. The <code>glide.ui.list_v3.enable</code> property must be set to <code>true</code> to enable the related list conditions builder.</td>
</tr>
<tr>
<td><code>glide.ui.list.related_list_search_filter</code></td>
<td>- Type: <code>true</code></td>
</tr>
<tr>
<td></td>
<td>- Default value: <code>true</code></td>
</tr>
<tr>
<td></td>
<td>- Location: <code>System Properties &gt; List v3</code></td>
</tr>
<tr>
<td></td>
<td>- Learn more: <a href="#">Add related list conditions</a></td>
</tr>
<tr>
<td>Lowering the value of <code>glide.ui.list.record watcher throttle</code> property</td>
<td>Time (ms) to wait between reacting to record watch events</td>
</tr>
<tr>
<td></td>
<td>- Type: <code>integer</code></td>
</tr>
<tr>
<td></td>
<td>- Default value: <code>30000</code></td>
</tr>
<tr>
<td></td>
<td>- Location: <code>System Properties &gt; List v3</code></td>
</tr>
<tr>
<td><code>glide.ui.list_v3.enable_live_related_lists</code></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>- Type: <code>true</code></td>
</tr>
<tr>
<td></td>
<td>- Default value: <code>true</code></td>
</tr>
<tr>
<td></td>
<td>- Location: System property (sys_properties) table</td>
</tr>
</tbody>
</table>

© 2019 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.
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

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><code>&lt;table&gt;.related_list_query.blacklist</code></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: <code>task_sla.task,task_ci.task</code></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.

![List v3 List Calculations window](image)
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 (_menu).
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.
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.
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.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>Contact type</td>
</tr>
<tr>
<td>Caller</td>
<td>State</td>
</tr>
<tr>
<td>Category</td>
<td>On hold reason</td>
</tr>
<tr>
<td>Subcategory</td>
<td>Impact</td>
</tr>
<tr>
<td>Business service</td>
<td>Urgency</td>
</tr>
<tr>
<td>Configuration item</td>
<td>Priority</td>
</tr>
<tr>
<td>Assignment group</td>
<td>Assigned to</td>
</tr>
</tbody>
</table>

- Short description
- Description
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 (赁) 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

You can add annotations to forms to display blocks of text or to add separators.
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.
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.
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:

1. Navigate to **System UI > Form Sections**.
2. 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.
3. Select the check box beside the form section to delete, and then select **Delete** from the **Actions on selected rows** menu.
4. 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 ( ) 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.
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.
### Change Request - CHG0000009

**Number**: CHG0000009

**Requested by**: Fred Luddy

**Category**: Software

**Configuration Item**: SAP ORA01

**Priority**: 1 - Critical

**Risk**: High

**Impact**: 3 - Low

**Approval**: Approved

**Type**: Comprehensive

**State**: Open

**Assignment group**: Bow Rugari

**Assigned to**: Bow Rugari

<table>
<thead>
<tr>
<th>Approver</th>
<th>Comments</th>
<th>Created</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bow Rugari</td>
<td></td>
<td>08-28-2014 23:31:50</td>
</tr>
<tr>
<td>David Lee</td>
<td></td>
<td>08-28-2014 23:31:50</td>
</tr>
<tr>
<td>Eric Schroeder</td>
<td></td>
<td>08-28-2014 23:31:51</td>
</tr>
<tr>
<td>Fred Luddy</td>
<td></td>
<td>08-28-2014 23:31:51</td>
</tr>
</tbody>
</table>
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 (ubah) 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 owned_by_indicator.form preference to true.</td>
</tr>
</tbody>
</table>
| Enable the indicator for an individual administrator | 1. Make sure the owned_by_indicator.form system user preference is set to false.  
  2. 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 ( ) 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

For evaluation, you can activate the plugin for an application that requires a purchased subscription on a non-production instance. To activate the plugin on production instances, you must purchase the subscription. To purchase a subscription, contact your ServiceNow account manager. For details on purchasing a plugin, see Purchase a plugin.

Some plugins require activation by ServiceNow personnel. Request these plugins through the HI Customer Service System instead of activating them yourself. For details, see Request a plugin.

For plugins that you can activate yourself, continue with the following steps.

1. Navigate to System Definition > Plugins.
2. Find and click the plugin name.
3. On the System Plugin form, review the plugin details and then click the Activate/Upgrade related link.
   - If the plugin depends on other plugins, these plugins are listed along with their activation status.
   - If the plugin has optional features that depend on other plugins, those plugins are listed under Some files will not be loaded because these plugins are inactive. The optional features are not installed until the listed plugins are installed (before or after the installation of the current plugin).
4. Optional: If available, 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 practice when you first activate the plugin on a development or test instance.
   - You can also load demo data after the plugin is activated by clicking the Load Demo Data Only related link on the System Plugin form.
5. Click Activate.

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.

The following information is entered 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>
<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.

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

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.

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.

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.

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. Click the Attributes tab.
4. Click New and add the following values.

<table>
<thead>
<tr>
<th>Attribute values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
</tr>
<tr>
<td>-------</td>
</tr>
<tr>
<td>Attribute</td>
</tr>
<tr>
<td>Value</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.
5. Click **Submit**.
   The indexing process begins. When it is complete, attachments can be searched on that table.

6. Optional: To disable attachment indexing, remove the attribute and click **Update**.

**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><strong>Select icon by</strong></td>
<td>Select MIME Type or File Extension.</td>
</tr>
</tbody>
</table>

**Note:** 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MIME type</strong></td>
<td>If <strong>Select icon by</strong> is <strong>MIME Type</strong>, enter the MIME type and subtype to associate with the icon, separated by a slash (example: application/pdf).</td>
</tr>
<tr>
<td><strong>File extension</strong></td>
<td>If <strong>Select icon by</strong> is <strong>File Extension</strong>, enter the file extension to associate with the icon beginning with the period (example: .pdf).</td>
</tr>
<tr>
<td><strong>Icon</strong></td>
<td>Enter the path to the icon image file (example: images/icons/attach_pdf.gifx)</td>
</tr>
</tbody>
</table>

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 flow formatter</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.
This Jelly script is reproduced below in plain text that you can copy into the Macro form as a basis for your macro script.

```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>
```

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 displays 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

Don Goodliffe
Server out of memory

Don Goodliffe
Added an attachment

Don Goodliffe
Moved to lane 'Doing' from 'To Do'

Don Goodliffe
Assigned to David Loo
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, a 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>
<tbody>
<tr>
<td>UI16</td>
<td>1. Click the activity filter icon ( ).&lt;br&gt;2. At the bottom of the list, click <strong>Configure available fields</strong>.</td>
</tr>
<tr>
<td>UI15</td>
<td>Right-click the <strong>Activity</strong> header and select <strong>Configure Activities</strong>.</td>
</tr>
</tbody>
</table>

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>Name</td>
<td>glide.ui16.emailStreamResponseActions</td>
</tr>
<tr>
<td>Description</td>
<td>Add the email reply button to the activity stream.</td>
</tr>
<tr>
<td>Type</td>
<td>true</td>
</tr>
<tr>
<td>Value</td>
<td>Set the value to true. 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
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 Definition > Plugins**.
2. Find and click the plugin name.
3. On the System Plugin form, review the plugin details and then click the **Activate/Upgrade** related link.
   - If the plugin depends on other plugins, these plugins are listed along with their activation status.
   - If the plugin has optional features that depend on other plugins, those plugins are listed under **Some files will not be loaded because these plugins are inactive**. The optional features are not installed until the listed plugins are installed (before or after the installation of the current plugin).
4. Optional: If available, 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 practice when you first activate the plugin on a development or test instance.
   - You can also load demo data after the plugin is activated by clicking the **Load Demo Data Only** related link on the System Plugin form.
5. Click **Activate**.

**Create a process flow formatter**

You can create a process flow formatter stage.

Role required: admin

1. Navigate to **System UI > Process Flow**.
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>
<tr>
<td>Active</td>
<td>Select the check box to ensure that the formatter stage is active.</td>
</tr>
<tr>
<td>Order</td>
<td>Enter a number to indicate where in the process flow the formatter will be displayed.</td>
</tr>
<tr>
<td>Condition</td>
<td>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.</td>
</tr>
<tr>
<td>Description</td>
<td>Describe the process flow formatter. This description does not appear on the actual formatter.</td>
</tr>
</tbody>
</table>

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(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></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Performance of the Siebel SFA software has been severely degraded since the upgrade performed this weekend.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>We moved to an unsupported Oracle DB version. Need to rollback the Oracle instance to a supported version.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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><strong>Option</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>glide.history.max_entries</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. Complete the form, as appropriate.
## Template form fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Display name of this template.</td>
</tr>
<tr>
<td>Table</td>
<td>Table this template applies to. Select <strong>Global</strong> to make the template available for use with all tables.</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 template.</td>
</tr>
<tr>
<td>Active</td>
<td>Option for making the template available for use. A template must be active to be used.</td>
</tr>
<tr>
<td>User</td>
<td>User who can configure and apply the template. If a user is defined, no other users can see the template unless the <strong>Global</strong> check box is selected.</td>
</tr>
<tr>
<td>Group</td>
<td>A group whose members can configure and apply the template. If a group is defined, no other groups can see the template unless the <strong>Global</strong> check box is selected.</td>
</tr>
<tr>
<td>Global</td>
<td>Option for allowing any user who can access templates to view and apply this template.</td>
</tr>
<tr>
<td>Short description</td>
<td>Description of the template. <strong>Note:</strong> Adding content to this field does not add that content to the <strong>Short description</strong> field of forms that use this template.</td>
</tr>
<tr>
<td>Template</td>
<td>The content that automatically populates records based on this template. Select a field from the specified table in the left column, then enter the data to automatically populate in the right column.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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>Link element</td>
<td>Links a template for 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. Once set, the child template is explicitly linked to the parent.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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>
</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>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 <strong>Self-Service</strong>, and click the edit application (pencil) icon.</th>
</tr>
</thead>
<tbody>
<tr>
<td>UI15</td>
<td>Right-click an application menu and select <strong>Edit Application Menu</strong>.</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 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>
</tbody>
</table>
### All Templates popup

This window displays when the **All Templates** button is selected. The window displays a filterable list of all available templates. Click the **Edit** button to the left of any template to edit that template.

### Disable Template Bar button ( )

Disables the template bar. To display the bar, see "Toggle the template bar".

---

**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**

1. Click the more options icon ( ) in the form header.
2. Select **Toggle Template Bar**.
1. Right-click the form header.
2. 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.assignment_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.
ServiceNow London Now Platform Administration

![Form UI actions](Image)

- **Form button**
- **Right-click form context menu**
- **Form link**

© 2019 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>#</th>
<th>Number</th>
<th>Short description</th>
<th>Approval</th>
<th>Type</th>
<th>State</th>
<th>Planned start date</th>
<th>Planned end date</th>
<th>Assigned to</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CH500000012</td>
<td>Java App Server</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>CH500000011</td>
<td>Another Java App Server change</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>CH500000010</td>
<td>Java Application change</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>CH500000009</td>
<td>Apply patches 10.2.6.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>CH500000008</td>
<td>Install newer Cisco</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>CH500000007</td>
<td>R&amp;D wants to move to Linux over to Linux desktops</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**List UI actions**

- List banner button
- Right-click list context menu
- List bottom button
- List choice
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.

### UI action fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Defines the text that appears on the button, link, or context menu item.</td>
</tr>
<tr>
<td><strong>Table</strong></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><strong>Order</strong></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><strong>Action name</strong></td>
<td>Defines a name to use when referencing the UI action in scripts.</td>
</tr>
<tr>
<td><strong>Active</strong></td>
<td>Enables the UI action when selected. To disable a UI action, clear the check box.</td>
</tr>
<tr>
<td><strong>Show insert</strong></td>
<td>Shows a button on new records that have not been inserted.</td>
</tr>
<tr>
<td><strong>Show update</strong></td>
<td>Shows a button on existing records.</td>
</tr>
<tr>
<td><strong>Client</strong></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 <strong>Condition</strong> field.</td>
</tr>
<tr>
<td><strong>List v2 Compatible</strong></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><strong>List v3 Compatible</strong></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><strong>Form button</strong></td>
<td>Puts a button on a form.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</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>
<tr>
<td>List banner button</td>
<td>Puts a button in the banner of a list.</td>
</tr>
<tr>
<td>List bottom button</td>
<td>Puts a button at the bottom of a list.</td>
</tr>
<tr>
<td>List context menu</td>
<td>Puts an item in a list field context menu (right-click a cell in a list).</td>
</tr>
<tr>
<td>List choice</td>
<td>Puts an item in the action choice list at the bottom of a list.</td>
</tr>
<tr>
<td>List link</td>
<td>Puts a link in the Related Links section at the bottom of a list.</td>
</tr>
<tr>
<td>Overrides</td>
<td>Specifies a UI action that this UI action overrides.</td>
</tr>
<tr>
<td>Comments</td>
<td>Provides descriptive content regarding this UI action.</td>
</tr>
<tr>
<td>Hint</td>
<td>Defines the text that appears when a user points to the UI action control.</td>
</tr>
<tr>
<td>Onclick</td>
<td>The name of the JavaScript function to run when the UI action is executed.</td>
</tr>
<tr>
<td>Condition</td>
<td>Defines the conditions that restrict when a UI action appears.</td>
</tr>
<tr>
<td>Script</td>
<td>Defines the script to run when the UI action is executed.</td>
</tr>
<tr>
<td>Related lists on the form view:</td>
<td>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.</td>
</tr>
<tr>
<td>Versions</td>
<td>Shows all versions of the UI action. Use this list to compare versions or to revert to a previous version.</td>
</tr>
</tbody>
</table>

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:

```java
action.setRedirectURL (new_record );
```

**Restricting UI actions based on conditions**

You can include scripts in the Condition field of the UI Action form. The condition must evaluate to `true` for the action to appear.

**Using the UI action condition builder**

If you leave the field empty, the condition defaults to `true`. For example, the following condition is configured for the **Close Incident** button:

```
Condition: current.incident.state == 6 && (gs.hasRole("itil_admin") || gs.getUserID() == current.caller_id)
```
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 check box 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.

---

**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>
<tr>
<td>When to Apply</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<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>
<tr>
<td>On load (Advanced view)</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• In the UI Policy Actions related list, creates a record that makes the Additional comments field mandatory when the condition is met.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Inherit (Advanced view)</td>
<td>Option for specifying whether extended tables inherit this UI policy.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Consider the following example:</td>
</tr>
<tr>
<td></td>
<td>- A child table has a UI policy with Order value 500 that shows the Urgency field when its conditions are met.</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td>Script</td>
<td></td>
</tr>
<tr>
<td>Run scripts (Advanced view)</td>
<td>Option for specifying whether advanced behavior can be scripted for both true and false conditions.</td>
</tr>
<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>
<tr>
<td>Other fields</td>
<td></td>
</tr>
<tr>
<td>Run scripts in UI type</td>
<td>The UI type for this UI policy: Desktop, Mobile / Service Portal, or Both.</td>
</tr>
<tr>
<td>Related List: UI Policy Actions</td>
<td>(read-only) Field the UI policy action applies to.</td>
</tr>
<tr>
<td>Table</td>
<td>Field on the selected table to which the UI policy performs an action if true.</td>
</tr>
<tr>
<td>Field name</td>
<td></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>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Mandatory  | Choice list for specifying how the UI policy affects the mandatory state of the field. Choices are:  
  - Leave alone  
  - True  
  - False |
| 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>
</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 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.');
}
```

Service catalog UI policies control the behavior of catalog item forms. Service catalog UI policies can be applied to a catalog item or a variable set. For more information about using UI policies for service catalog items, see **Service catalog UI policy**

**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 screen readers 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. Add a property with the following settings.

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>glide.ui.show_template_bar.&lt;TABLENAME&gt;</td>
</tr>
<tr>
<td>Type</td>
<td>true</td>
</tr>
<tr>
<td>Value</td>
<td>false</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.
```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`).

### 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

- begin_split -
Asset tag
State
- split -
Serial number
Substate
- end_split -
- begin_split -
Assigned to
Stockroom
Reserved for
Managed by
Owned by
Parent
Class
- split -
Location
Department
Company
Assigned
Installed
- end_split -
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](image)

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.

Choose the **Caller** field and click the expander icon.

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.

---

**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.

---

## Field types

<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>
</tbody>
</table>
| Color        | String field that accepts CSS color declarations (including hex or RGB notation) and displays a preview. See:  
  * [HTML Colors (W3Schools)](https://www.w3schools.com/html/html_colors.asp) for more information on hex and RGB notation.  
  * [HTML Color Names (W3Schools)](https://www.w3schools.com/html/html_color_names.asp) for valid color names. |
<p>| Condition String | Text field that accepts a plain JavaScript condition statement that is validated automatically for correctness before an update. |</p>
<table>
<thead>
<tr>
<th>Field Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
<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 <a href="#">Change currency decimal places</a> for how to use two fraction digits.</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>HTML</td>
<td>String field with a built-in HTML editor.</td>
</tr>
<tr>
<td>Field Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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 <a href="https://servicenow.com/IMG/blueprint/field.html#ip-address">IP address field type</a> 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>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>For information on scripting Name-Value Pairs fields, see <a href="https://servicenow.com/IMG/blueprint/field.html#name-value-pairs">Name-value pairs field type</a>.</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>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 <a href="https://servicenow.com/IMG/blueprint/field.html#encryption-contexts">Encryption Contexts</a>. 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>Field Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</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 <a href="#">Price fields</a> 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>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The database may translate the value 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).</td>
</tr>
<tr>
<td></td>
<td>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>
</tbody>
</table>
| String (Full UTF-8)     | 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. &
<p>|                         | 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. |
| Suggestion              | 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. |
| Table Name              | 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. |</p>
<table>
<thead>
<tr>
<th>Field Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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 based on the user's language.</td>
</tr>
<tr>
<td>Translated Text</td>
<td>Text field that displays different translations based on the user's language.</td>
</tr>
<tr>
<td>True/False</td>
<td>Boolean field that appears as a check box.</td>
</tr>
<tr>
<td>URL</td>
<td>String field that is a clickable URL field when locked.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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.</td>
</tr>
<tr>
<td>Video</td>
<td>Field for uploading and embedding video.</td>
</tr>
<tr>
<td>Wiki</td>
<td>String field with a built-in Wiki text editor that accepts a simplified version of standard Wiki text formatting.</td>
</tr>
<tr>
<td>Workflow</td>
<td>Choice list field that displays a stage in a workflow.</td>
</tr>
</tbody>
</table>

**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.
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.

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.
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 provides 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.

<table>
<thead>
<tr>
<th>Value</th>
<th>Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>New</td>
</tr>
<tr>
<td>2</td>
<td>Active</td>
</tr>
<tr>
<td>3</td>
<td>Awaiting Problem</td>
</tr>
<tr>
<td>4</td>
<td>Awaiting User Info</td>
</tr>
<tr>
<td>5</td>
<td>Awaiting Evidence</td>
</tr>
<tr>
<td>6</td>
<td>Resolved</td>
</tr>
<tr>
<td>7</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>
</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**.
4. Navigate again to **System Definition > Choice Lists**.
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
```
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)**.

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>Label</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 Time zone choice list in a user record to use the time zone value of the instance.</td>
</tr>
<tr>
<td>Value</td>
<td>Enter NULL_OVERRIDE.</td>
</tr>
<tr>
<td>dependent</td>
<td>Leave blank.</td>
</tr>
<tr>
<td>hint</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](image)

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) older instances may have (12,2)</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></td>
<td>&lt;reference table&gt;</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 glide duration to a glide datetime since both logical data types map to the DATETIME physical data type in the database.</td>
</tr>
</tbody>
</table>
### Condition | Restrictions
--- | ---
The field is a string field you are converting to another type of string field. | 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.
The field is a string field you are converting to a globally unique ID (GUID). | You can only convert a string field to a GUID if all of the exiting data in the field are already Sys ID values.
The field is a GUID field you are converting to a string field. | None. You can convert a GUID field to a string field without restriction.

### 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.
**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.

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, justifyleft, justifycenter, justifyright, justifyfull, formatselect, fontselect, fontsize, 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>
<tr>
<td>Extended functions</td>
<td>link, unlink, cleanup, code, hr, visualaid, charmap, image, media, preview, spellchecker, fullscreen (not supported by Internet Explorer)</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Button purpose</th>
<th>Accepted button names</th>
</tr>
</thead>
<tbody>
<tr>
<td>Formatting</td>
<td>formatblock, fontname, fontsize, bold, italic, underline, justifyleft, justifycenter, justifyright, justifyfull, insertorderedlist, insertunorderedlist, outdent, indent, forecolor, hilitecolor</td>
</tr>
<tr>
<td>Editing</td>
<td>copy, paste, undo</td>
</tr>
<tr>
<td>Extended functions</td>
<td>createlink, inserthorizontalerule, insertimage, insertvideo, inserttable, htmlmode</td>
</tr>
</tbody>
</table>

4. Click **Save**.
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><strong>B</strong></td>
<td><strong>B</strong></td>
<td><strong>Bold</strong></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><strong>I</strong></td>
<td><strong>I</strong></td>
<td><strong>Italic</strong></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><strong>U</strong></td>
<td><strong>U</strong></td>
<td><strong>Underline</strong></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><strong>Align Right</strong></td>
<td><strong>Align Right</strong></td>
<td><strong>Align Right</strong></td>
<td>Applies right alignment to the current paragraph.</td>
</tr>
<tr>
<td><strong>Align Center</strong></td>
<td><strong>Align Center</strong></td>
<td><strong>Align Center</strong></td>
<td>Applies center alignment to the current paragraph.</td>
</tr>
<tr>
<td><strong>Align Left</strong></td>
<td><strong>Align Left</strong></td>
<td><strong>Align Left</strong></td>
<td>Applies left alignment to the current paragraph.</td>
</tr>
</tbody>
</table>

© 2019 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>htmlArea icon</th>
<th>TinyMCE icon</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
|              |              | Justify | Applies justified alignment, which stretches the lines to equal width, to the current paragraph.  
  **Code reference:** `text-align: justify` |
| Paragraph     |              | Format | Applies a paragraph style to the current paragraph, such as Paragraph, Heading 1, and Preformatted. |
| Arial         | Font Family  | Font Family | Applies a font family to the selected text or current word. |
| 3 (12pt)      | Font Sizes   | Font Size | Applies a font size to the selected text or current word. |
|               |              | Insert/Remove Bulleted List | Applies or removes unordered list tags for the selected paragraphs. Click the arrow beside the button to select a different bullet type. |
|               |              | Insert/Remove Numbered List | Applies or removes ordered list tags for the selected paragraphs. Click the arrow beside the button to select a different number type. |
|               |              | Decrease Indent | Removes indentation from the current or selected paragraphs (removes 30px of left padding; padding cannot be less than 0).  
  **Code reference:** `padding-left` |
|               |              | Increase Indent | Applies indentation to the current or selected paragraphs (adds 30px of left padding).  
  **Code reference:** `padding-left` |
<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<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 <strong>More Colors...</strong> 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 <strong>More Colors...</strong> to view various color options and the hexadecimal codes.</td>
</tr>
</tbody>
</table>

**Extended functions**
The extended functions available for working with HTML content.

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<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). &lt;a&gt;</td>
</tr>
<tr>
<td>Remove link*</td>
<td>Removes the current hyperlink.</td>
</tr>
<tr>
<td>Cleanup Messy Code*</td>
<td>Fixes standard HTML errors for the selected text, such as invalid tags. Clicking this button may change the layout of existing content. If you do not like the results, you can click <strong>Undo</strong> to revert this action.</td>
</tr>
<tr>
<td>Icon</td>
<td>TinyMCE v4 Icon</td>
</tr>
<tr>
<td>------</td>
<td>----------------</td>
</tr>
<tr>
<td>HTML</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Icon</td>
<td>TinyMCE v4 Icon</td>
</tr>
<tr>
<td>------</td>
<td>----------------</td>
</tr>
<tr>
<td><img src="image" alt="Toggle Full Screen Mode" /></td>
<td><img src="image" alt="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><img src="image" alt="Cut" /></td>
<td><img src="image" alt="Cut" /></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><img src="image" alt="Copy" /></td>
<td><img src="image" alt="Copy" /></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><img src="image" alt="Paste" /></td>
<td><img src="image" alt="Paste" /></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><img src="image" alt="Paste as Plain Text" /></td>
<td><img src="image" alt="Paste as Plain Text" /></td>
<td>Paste as Plain Text*</td>
<td>Enables paste as plain text without source formatting.</td>
</tr>
<tr>
<td><img src="image" alt="Paste from Word" /></td>
<td><img src="image" alt="Paste from Word" /></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>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="image1" alt="Find Icon" /></td>
<td><img src="image2" alt="Find V4 Icon" /></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>
<tr>
<td><img src="image3" alt="Find/Replace Icon" /></td>
<td><img src="image4" alt="Find/Replace V4 Icon" /></td>
<td>Find/Replace*</td>
<td>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</td>
</tr>
<tr>
<td><img src="image5" alt="Undo Icon" /></td>
<td><img src="image6" alt="Undo V4 Icon" /></td>
<td>Undo*</td>
<td>Reverts the previous edit.</td>
</tr>
<tr>
<td><img src="image7" alt="Redo Icon" /></td>
<td><img src="image8" alt="Redo V4 Icon" /></td>
<td>Redo*</td>
<td>Reapplies the last reverted edit.</td>
</tr>
</tbody>
</table>

*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>
</table>
| ![Table Icon](image9) | Click the table icon (Insert table) to access the TinyMCE version 4 table menu. Use the table menu to:  
  - Insert or delete a table  
  - Modify table properties  
  - Add, move, or delete rows and columns  
  - Modify row and column properties  
  - Split and merge cells |

© 2019 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.
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
With the cursor in the desired table cell, open the table menu and click **Cell properties**. From this box you can set the following properties for table cells.

- **General tab:**
  - Width and height
  - Type and scope
  - Horizontal and vertical alignment

- **Advanced tab**
  - Configure the cell style
  - Select the border color
  - Select the background color

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.

- **Row type**
- **Alignment**
- **Height**

- **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.

**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](image)

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 **#87cefa** 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
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>Type</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>
</tbody>
</table>

© 2019 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 | Description
--- | ---
**Image** | Begin typing a file name and select an image from the list, or click the reference lookup icon and select an image. To upload a new image, click **New**, click **Choose File**, locate the image, and click **Upload**. If you chose the **Attachment** type, click **Choose File**, locate the image, and click **Attach**.

**Tooltip** | Enter alternate text that appears when a user points to the image.

**Alt** | 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 **Tooltip** field.

---

**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.
ServiceNow    London    Now Platform Administration

Insert/Edit Link form

<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>
<tr>
<td></td>
<td>For files, the <strong>None (use implicit)</strong> selection is generally the best choice. However, if you are linking to a complete web page, choose <strong>New window (_blank)</strong> so the browser opens the link in a new tab or window.</td>
</tr>
</tbody>
</table>

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 will start. To reduce file size, you can reduce the bitrate, but doing so reduces the quality of the video. The following bitrates 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 to 2.5 megabits per second (mbps)</td>
</tr>
<tr>
<td>High definition (720p)</td>
<td>3 to 5 mbps</td>
</tr>
<tr>
<td>High definition (1080p)</td>
<td>6 to 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 form

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>Select the video type.</td>
</tr>
<tr>
<td>- Video Library: List of videos stored in the db_video table. May be reused.</td>
<td></td>
</tr>
<tr>
<td>- URL: from an external source</td>
<td></td>
</tr>
<tr>
<td>- Attachment: available in the current record only</td>
<td></td>
</tr>
</tbody>
</table>

For an attachment or video library file, select a video from the list or click **New**. For an external URL, enter the URL.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Size</strong></td>
<td>Enter the <strong>Width</strong> and <strong>Height</strong> of the video in pixels.</td>
</tr>
</tbody>
</table>

5. **Click OK.**

By default, the HTML Sanitizer removes videos from HTML fields. To prevent the video from being removed:

- Add an attribute to the text field on the form that the video is added to:
  ```javascript```

```javascript
html_sanitize=false.
```

Adding the attribute stops this HTML field from being sanitized in the future.

- Modify the white list in the script include `HTMLSanitizerConfig` to add the embed, object, and param attributes. The script include allows the attributes to be used in all HTML fields in the future. For example:

```javascript
HTML_WHITELIST:{
  globalAttributes: {
    // attribute:
    // attributeValuePattern: {}
  },
  embed: {attribute:
    // src, type, allowfullscreen, allowscriptaccess, plugnspace
  },
  object: {attribute:
    // classid, codebase
  },
  param: {attribute:
    // name, value
  }
}
```

- Universally override elements that the TinyMCE strips out by adding a list of elements to the `glide.ui.html.editor.extended_valid_elements` property. For example, add `[onclick|href|target|rel|media[hreflang]type|charset|name[rev|shape|coords|download]id|accesskey|class|dir|lang|style|tabindex|title]` to the system property.

### 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 white list 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 Plugins page 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.

   ```
   <j:if test= "${jvar_use_dbimage}"
   <j:set var = "jvar_default_insert_image_type" value = "dbimage" />
   <g:ui_select_option text = "${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) 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:f0d0:1002:0051:0000:0000:0000:0004
- 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 dot-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</td>
<td>Specifies the number of entries from a journal field (such as Additional comments and Work notes) included in email notifications (-1 means all). Type: integer, Default value: 3, 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
var notes = current.work_notes.getJournalEntry(-1);
// gets all journal entries as a string where each entry is delimited by '
 \n' var na = notes.split("\n\n");

// stores each entry into an array of strings
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 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`

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:

<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/blogs/blogging/product-development/service-now-technical-support-enginers) by a ServiceNow Technical Support Engineer in the ServiceNow 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).
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/blogs/blogging/product-development/service-now-technical-support-enginers).
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.

---

**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.

---

**Note:** 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.

---

**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 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>
<tr>
<td>65</td>
<td>59</td>
<td>90.7%</td>
<td>lightgreen</td>
</tr>
<tr>
<td>15</td>
<td>10</td>
<td>66.7%</td>
<td>khaki</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.

Phone e164

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.

Phone e164 strict

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.

Phone e164 not strict

**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.

Phone e164 entry local

Phone e164 display international

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.
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>
<tbody>
<tr>
<td>glide.phone_number_e164.display_territory_selector</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>* Type: true</td>
</tr>
<tr>
<td></td>
<td>* Default value: true</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_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>
</tbody>
</table>
### Property Description

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>read-only</strong></td>
<td>displays the territory label in read-only mode, regardless of whether the number is in local or international format.</td>
</tr>
<tr>
<td><strong>read-only-national</strong></td>
<td>displays the territory label in read-only mode only if the number is in local format.</td>
</tr>
<tr>
<td><strong>list</strong></td>
<td>displays the territory label in a list.</td>
</tr>
<tr>
<td><strong>list-national</strong></td>
<td>displays the territory label in a list if the number is in national format.</td>
</tr>
<tr>
<td><strong>none</strong></td>
<td>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:

<table>
<thead>
<tr>
<th>Dictionary attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pn_display_territory_text</td>
<td>Overrides the glide.phone_number_e164.display_territory_text property that defines when a phone number field displays a territory label. Available values are identical to those described above for the glide.phone_number_e164.display_territory_text 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 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)

E164 phone display idd

**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:
Dictionary attribute | Description
--- | ---
*pn_display_users_idd* | 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.
- **Type**: true | false
- **Default value**: false
- **Example**: `pn_display_users_idd=false`

### 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>
</table>
| `glide.phone_number_e164.strict` | Determines whether all phone number fields must match the display format for the selected territory. When the value is **true**, 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 **false**, 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.

- **Type**: true | false
- **Default value**: true
- **Location**: Add to the System Properties (sys_properties) table.
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| glide.phone_number_e164.allow_national_entry | Determines whether users can enter phone numbers in the local format or whether they must enter phone numbers in international format. When **true**, users can enter phone numbers in the local format for the selected territory. When **false**, users must enter phone numbers in the international format for the selected territory.  
  * **Type**: true | false  
  * **Default value**: true  
  * **Location**: Add to the System Properties (sys_properties) table. |
| glide.phone_number_e164.display_national | Determines whether to display E.164 phone numbers in local format.  
  * **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  
  * **Location**: Add to the System Properties (sys_properties) table. |
<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>
Dictionary attribute | Description
--- | ---
pn_display_users_idd | 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.
  - Type: true | false
  - Default value: false
  - Example: `pn_display_users_idd=false`

### 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:

1. Navigate to **System Policy > Rules > Telephone Display Rules**.
2. Click a territory **Name**.
3. Edit the fields, as appropriate (see table).
4. Click **Update**.
## 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>
</tbody>
</table>
### Order

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.

### 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 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.

**Note:** A reference field can refer only to records from one other table. To add a field that can refer to records on any table, use the Document ID element type.

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>
</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) {
```
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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Clear or -- None --</strong></td>
<td>Deleting a record clears references (default option).</td>
</tr>
<tr>
<td><strong>Delete or Cascade</strong></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.</td>
</tr>
<tr>
<td><strong>Restrict</strong></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><strong>None</strong></td>
<td>Deleting a record does not change records that reference the record.</td>
</tr>
</tbody>
</table>

**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.

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.
Display value xml

Reference field

<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</td>
<td>46b87022a9fe198101a78787e40d7547</td>
<td>ref Woo (sys_user.name)</td>
<td>Charlie Whitherspoon</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.
Note: If you make a field the display field for a table, be sure to translate all values for the field in the Translated Text (sys_translated_text) table into all the languages provided. Display field options left untranslated are not presented by the autocomplete (type ahead) feature.

Reference fields look for the display value in the following order:

1. A field with display=true in the system dictionary on the lowest sub-table for extended tables.
2. A field with display=true in the system dictionary on the parent table.
3. A field named name or u_name.
4. 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

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 (<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 styles**

Reference styles are specialized field styles that control the appearance of reference fields.

For more information, see [Define reference styles](#).

**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 JavaScript, 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 qual 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 another example, if you are trying to filter based on the current company, you don't have to use a lookup script but can simply add this line to your dynamic qualifier:

```
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(){
    // ...
}
```
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.
### Field Table

<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>
| 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
   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 gr = new GlideRecord('sys_user_has_role');
if (roleListIds) {
  gr.addQuery('role', queryCondition, roleListIds);
}
gr.query();
while (gr.next()) {
  users[gr.user.toString()] = true;
}

var ids = [];
for (var id in users)
  ids.push(id);

return ids;

// get sys_id's for the named roles
function getRoleListIds(roleList) {
  var ids = [];
  var gr = new GlideRecord('sys_user_role');
  gr.addQuery('name','IN',roleList);
  gr.query();
  while (gr.next()) {
    ids.push(gr.sys_id.toString());
  }

  return ids;
}

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 BackfillAssignmentGroup().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 Client callable option is selected and that the Accessible form field is properly set for the environment.

var BackfillAssignmentGroup = Class.create();
BackfillAssignmentGroup.prototype = {
  initialize: function() {
  },

BackfillAssignmentGroup:function() {
  var gp = ' '; 
  var a = current.assigned_to;

  //return everything if the assigned_to value is empty
  if(!a)
    return;
  //sys_user_grmember has the user to group relationship
var grp = new GlideRecord('sys_user_grmember');
grp.addQuery('user',a);
grp.query();
while(grp.next()) {
  if (gp.length > 0) {
    //build a comma separated string of groups if there is more than one
    gp += (',' + grp.group);
  } else {
    gp = grp.group;
  }
} // return Groups where assigned to is in those groups we use IN for lists
return 'sys_idIN' + gp;
},
type: 'BackfillAssignmentGroup'
}

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.

```plaintext
sys_class_nameINSTANCEOFcmdb_ci_server
```

In another example, you can simplify the following reference qualifier in a similar way.

```plaintext
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.

```plaintext
u_active=true^sys_class_name=cmdb_ci_acc
^ORsys_class_nameINSTANCEOFcmdb_ci_server
^ORsys_class_name=cmdb_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>
<tbody>
<tr>
<td>ref_auto_completer</td>
<td>Specifies the name of the client-side JavaScript class that creates the drop-down auto-completion choices. Valid class values include:</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td>ref_ac_columns</td>
<td>Specifies the list of reference table columns to display. Separate 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.</td>
</tr>
<tr>
<td>ref_ac_columns_search</td>
<td>Enables auto-complete to match text in the columns listed in the ref_ac_columns attribute. Set this attribute to <strong>true</strong> to enable auto-complete to match text in all reference field columns. By default (or when this attribute is <strong>false</strong>) auto-complete only matches text in the display value column.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ref_ac_order_by</td>
<td>Specifies the reference table column that sorts the auto-completion choices. For example, ref_ac_order_by=\textit{name} sorts the auto-completion choices alphabetically by name.</td>
</tr>
</tbody>
</table>

Administrators can also set a user preference to use a \textit{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.

**Selected row highlight**

Set the \texttt{ref_auto_completer=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

© 2019 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.
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 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, 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.

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.

Note: Auto-complete cannot match text from additional columns when the reference field is a product of the ui_reference UI macro. This means any auto-complete action against a selector, such as the Impersonate User list, can only match text against the display value.

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.
### Version v2
**List v2**
Right-click the column header and click **Configure > Dictionary**.

### Version v3
**List v3**
Open the list title menu and click **Configure**, and then click **Dictionary**.

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, 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_columns_search=true,ref_ac_display_value=false
   ```

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](image)

**Assigned to**

<table>
<thead>
<tr>
<th>James</th>
<th>Johnson</th>
</tr>
</thead>
</table>

**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.
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.

---

**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.
3. Under **Related Links**, click **Advanced view**.
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.
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.
Recent selections filtered

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_dictionary

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><strong>&quot;text&quot;</strong></td>
</tr>
<tr>
<td>Italic</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> &lt;link text&gt;)</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</td>
</tr>
<tr>
<td></td>
<td>&lt;b&gt;bold&lt;/b&gt;, &lt;strong&gt;strong&lt;/strong&gt;,</td>
</tr>
<tr>
<td></td>
<td>&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;,</td>
</tr>
<tr>
<td></td>
<td>&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 
\[
\text{[[INC0000002]]}
\].

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 <a href="#">W3Schools article</a>.</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 Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>🌟 Add the current user</td>
<td>Add the current user</td>
</tr>
<tr>
<td>✗ Remove the highlighted user</td>
<td>Remove the highlighted user</td>
</tr>
<tr>
<td>📝 Open the highlighted user's record (active only when a user record exists)</td>
<td>Open the highlighted user's record (active only when a user record exists)</td>
</tr>
<tr>
<td>🔉 Open a slushbucket to add or remove multiple users (not available until a record has initially been saved)</td>
<td>Open a slushbucket to add or remove multiple users (not available until a record has initially been saved)</td>
</tr>
<tr>
<td>🥗 Collapse or expand the watch list</td>
<td>Collapse or expand the watch list</td>
</tr>
<tr>
<td>Icon</td>
<td>Function</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
</tr>
<tr>
<td><img src="image" alt="icon" /></td>
<td>Open a reference list to select a single user</td>
</tr>
<tr>
<td><img src="image" alt="icon" /></td>
<td>Enter an email address for users who are not in the User (sys_user) table or do not have an email address defined in their user record</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**.

**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. 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.

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><strong>Field</strong></th>
<th><strong>Input Value</strong></th>
</tr>
</thead>
</table>
| Table     | Table that contains the field.  
  
  **Note:** The list shows only tables and database views that meet the scope protections for field styles. |
| Field name| The field to which the style applies. |
| Value     | The exact value or script-based-condition required to apply the style.  
  
  **Note:** The value only affects list field styles. To apply field styles on both lists and forms, leave this field blank. |
| Style     | 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.  
  
  ```javascript
  background-color:red;  
  font-size:24px;  
  color:white;
  ```

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.

### Define reference styles

Reference styles are similar to field styles, but apply to any reference to a table. You can define styles that apply to any reference to a table.

Role required: admin

For instance, a reference style on the User (sys_user) table would apply to any reference field on any table that refers to User.

1. Enter `sys_ui_reference_style.list` in the application navigator filter and press Enter.
2. Click New.
3. Complete the form.

#### Reference Style form fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>If the check box is selected, the style is applied where appropriate.</td>
</tr>
<tr>
<td>Table</td>
<td>The table to which all references will be styled. Note: The list shows only tables that meet the scope protections for table styles.</td>
</tr>
<tr>
<td>Style</td>
<td>A CSS style to apply.</td>
</tr>
</tbody>
</table>

See Application scope.

### Modify string field length

You can modify the maximum character limit for a string field.

Role required: personalize_dictionary

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.
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:
  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:
  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.
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 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.

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 table

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Number</th>
<th>Number of digits</th>
<th>Table</th>
<th>Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGCT</td>
<td>10,000</td>
<td>7</td>
<td>Account</td>
<td>2016-01-08 10:21:57</td>
</tr>
<tr>
<td>ADOBE</td>
<td>10,000</td>
<td>7</td>
<td>Adobe Software License</td>
<td>2005-09-25 18:21:25</td>
</tr>
<tr>
<td>AINS</td>
<td>10,000</td>
<td>7</td>
<td>Assessment Instance</td>
<td>2013-04-08 13:38:01</td>
</tr>
<tr>
<td>APP</td>
<td>1,000</td>
<td>7</td>
<td>Appointment Booking</td>
<td>2017-06-01 16:47:27</td>
</tr>
<tr>
<td>ASG</td>
<td>10,000</td>
<td>7</td>
<td>Assessment Group</td>
<td>2013-04-19 13:03:03</td>
</tr>
</tbody>
</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: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: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, <strong>INC</strong> for Incident).</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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>
<tr>
<td>Number of digits</td>
<td>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).</td>
</tr>
</tbody>
</table>

**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
   padCurrentCategory();
   function padCurrentCategory() {
     var target = new GlideRecord(current.category + "");
     if (!target.isValidField("u_number") || target.isValidField("number"))
       return;
     var nm = new UNumberManager();
   }
   ```
3. Duplicate the base system script include named `NumberManager`.
4. Change the following two lines as indicated:

   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: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.

The result of the configuration in the image is an Incident number that is left padded.
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 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 Definition > Plugins.
2. Find and click the plugin name.
3. On the System Plugin form, review the plugin details and then click the Activate/Upgrade related link.
   - If the plugin depends on other plugins, these plugins are listed along with their activation status.
   - If the plugin has optional features that depend on other plugins, those plugins are listed under Some files will not be loaded because these plugins are inactive. The optional features are not installed until the listed plugins are installed (before or after the installation of the current plugin).
4. Optional: If available, 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 practice when you first activate the plugin on a development or test instance.
   - You can also load demo data after the plugin is activated by clicking the Load Demo Data Only related link on the System Plugin form.
5. Click Activate.

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>Preference</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable field normalization</td>
<td>This preference enables or disables the Field Normalization functionality, including transformations.</td>
</tr>
<tr>
<td>Preference</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable field normalization auditing</td>
<td>This preference enables or disables auditing of field normalization tables.</td>
</tr>
<tr>
<td>Logging</td>
<td>Select the maximum level of logging detail desired. For example, select Error to log only errors and Information to log errors, warnings, and information.</td>
</tr>
<tr>
<td>Decoration URL</td>
<td>Enter the URL for the help/information link associated with the Field Normalization decoration. This link opens the page presented to users who do not have rights to see the normalization or transformation record. The default link opens a ServiceNow Wiki page with a general explanation of Field Normalization. The purpose of this page is to explain to normal users why a field value they entered was changed automatically.</td>
</tr>
<tr>
<td>Restrict decorations to roles</td>
<td>Use this preference to define the user roles that can view the reference icon (decoration) adjacent to a normalized field. This decoration displays transformation and normalization records to users with the normalizer role. For all other users, it opens the URL specified in the Decoration URL preference. If this preference does not specify any roles, then all roles can see the decoration.</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_transformchooser</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.
The image shows a screenshot of the ServiceNow Now Platform Administration interface. It appears to be a configuration screen for a string field, with options to use for normalize and transform. The transform category is set to "Text," and there are several transform definitions available, including Left, Right, Constant, and Trim.
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 rollback option to revert changes after the job completes. By default, the system provides these data jobs.

<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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The system runs this job whenever you insert or update a field normalization record. Since this data job does not change any field values,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>there is no rollback option.</td>
</tr>
<tr>
<td>Normal value change</td>
<td>Normalization</td>
<td>Run this job to re-run field normalization and update field values when you change a normal value. The system creates this job whenever you</td>
</tr>
<tr>
<td></td>
<td></td>
<td>change a normal value. Rollback the data job to revert 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. Rollback</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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. Rollback the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>data job to revert normalized fields to their previous values.</td>
</tr>
<tr>
<td>Coalesce to normal</td>
<td>Normalization</td>
<td>Run this job to normalize reference field values by replacing references to multiple duplicate records with one reference to a normalized</td>
</tr>
<tr>
<td></td>
<td></td>
<td>record. The system creates this job whenever you change a normal value that applies to a reference field. Rollback the data job to restore</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the duplicate records as valid options. The rollback does not restore references to the previous records.</td>
</tr>
<tr>
<td>Transform application</td>
<td>Transformation</td>
<td>Run this job to transform all field values that match the transformation conditions. You cannot start this job while the Transformation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>record is in Test mode. The system creates this job whenever you create or update a transformation record. Rollback the data job to revert</td>
</tr>
<tr>
<td></td>
<td></td>
<td>transformed fields to their previous values.</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 <strong>Normalized Queries</strong> 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 <strong>Coalesce Normal Values</strong> for details.</td>
</tr>
<tr>
<td>Raw field</td>
<td>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 <strong>Creating a Raw Field</strong>.</td>
</tr>
</tbody>
</table>
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.

© 2019 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.
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.

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.
   1. Select the check box next to a job, and then select **Start** from the Actions menu.
   2. To run all data jobs at once, select all the check boxes, and then select the **Start** action.
   3. 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:
Field normalization rule fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name for this rule. For example, this name might be Xeon CPU Type.</td>
</tr>
<tr>
<td>Order</td>
<td>Order in which this rule should be evaluated. The platform parses the rules in the order configured until it finds one that evaluates to true.</td>
</tr>
<tr>
<td>Active</td>
<td>Enables or disables this rule. By default, new rules are active (true)</td>
</tr>
<tr>
<td>Make alias</td>
<td>If this check box is selected, and the rule evaluates to true, the rule makes an alias automatically from a pending value. If this check box is not selected, and the rule evaluates to true, the platform automatically changes the value for the named field in the record to the normal value, but does not create an alias.</td>
</tr>
<tr>
<td>Case sensitive</td>
<td>All pending values for the named field must match the case of the same value in a rule to be normalized.</td>
</tr>
<tr>
<td>Rule</td>
<td>Use the ServiceNow rule builder to construct the rules for normalizing fields. Rules automate the transformation of large numbers of pending field values into aliases.</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. <strong>Note:</strong> 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 <strong>TO TARGET</strong> 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.</td>
</tr>
<tr>
<td>Mode</td>
<td>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>.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</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 <a href="#">Create a raw field</a>.</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:**

<table>
<thead>
<tr>
<th>Text Transform that modify the text of the value.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Change Case</strong></td>
</tr>
<tr>
<td><strong>Constant</strong></td>
</tr>
<tr>
<td><strong>Delete</strong></td>
</tr>
<tr>
<td><strong>Insert</strong></td>
</tr>
<tr>
<td><strong>Left</strong></td>
</tr>
<tr>
<td><strong>Prefix</strong></td>
</tr>
<tr>
<td><strong>Replace</strong></td>
</tr>
<tr>
<td><strong>Right</strong></td>
</tr>
<tr>
<td><strong>Substring</strong></td>
</tr>
<tr>
<td><strong>Suffix</strong></td>
</tr>
<tr>
<td><strong>Trim</strong></td>
</tr>
</tbody>
</table>

**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.

   ![Transformation record](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 **Transform 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.
    
    ![Test Transform](image)
  
    d) Click **OK**.
    
    The platform transforms the raw value in the **Transformed data** field.
    
    ![Test Transform](image)
  
    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**. |
### Transform Type | Category | Description | Parameters
--- | --- | --- | ---
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 4, 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 4, 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 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 to 4 by a rounding interval of 1.0.  

© 2019 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.
Transform Type | Category | Description | Parameters
--- | --- | --- | ---
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

### 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.
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.

<table>
<thead>
<tr>
<th>Position parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Positive positions</td>
<td>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.</td>
</tr>
</tbody>
</table>
Negative positions

<table>
<thead>
<tr>
<th>Negative positions</th>
<th>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.</th>
</tr>
</thead>
</table>

Regex

<table>
<thead>
<tr>
<th>Regex</th>
<th>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).</th>
</tr>
</thead>
</table>

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.
Function:
```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.
Transformation regex example

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.

Transformation Regex 3

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.

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 polices 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.
   - 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>The table to which this policy 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 data policy.</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>Field</th>
<th>Description</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>
</tbody>
</table>
| Read Only | How the data policy affects the read only state of the field. Choices are:  
  - Leave alone  
  - True  
  - False |
| Mandatory | How the data policy affects the mandatory state of the field. Choices are:  
  - Leave alone  
  - True  
  - False |

**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.

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.
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>Urgency</td>
</tr>
<tr>
<td>1 - High</td>
<td>1 - High</td>
</tr>
<tr>
<td>1 - High</td>
<td>2 - Medium</td>
</tr>
<tr>
<td>1 - High</td>
<td>3 - Low</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>Beth Anglin</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Assignment Group</td>
</tr>
<tr>
<td>Fred Luddy</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>VIP Issues</td>
</tr>
</tbody>
</table>

Note: Each row in a data lookup table must be unique.

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.

Data lookup definitions fields

<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>
</tbody>
</table>
Field | Description
--- | ---
Run on form change | 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.

**Note:** This does not include changes automatically made by other data lookup rules, such as the Priority Lookup Rules.

Run on insert | Select this check box to automatically look up values whenever a user creates a new record.

Run on update | Select this check box to automatically look up values whenever a user saves or updates a record.

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.

<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>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.

---

© 2019 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.
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 u_vip_caller_lookup.</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>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</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>
<tr>
<td>Condition</td>
<td>Condition builder that sets the conditions for applying this state model to records. For example, you could add the condition <em>Category is Networking</em> versus <em>Category is Security</em> if there are different state models for networking requests and security requests.</td>
</tr>
<tr>
<td>Common Exit Condition</td>
<td>Condition builder that sets any common condition required for moving from one state to another.</td>
</tr>
</tbody>
</table>

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 <strong>Description</strong> 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>
</tbody>
</table>
### 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 Configure 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>(sys_state_model)</td>
</tr>
<tr>
<td></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>State Model</td>
<td>(sys_state_model)</td>
</tr>
<tr>
<td></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>
</tbody>
</table>

**Roles installed with State Model**

State Model adds the following role.

<table>
<thead>
<tr>
<th>Role Name</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 display and calculations of currency values.

A currency field holds a value, a currency code, and a reference currency value.

- The currency code is a three-letter ISO code that identifies the currency in which the value is specified.
- The reference currency value is a number representing the currency value in the reference currency. The reference currency value is calculated by a rate conversion when the currency value is saved.

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

The system locale is set using the `glide.system.locale` property. The value is in 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. The system locale should be set once on a fresh zboot because reference currency values in currency fields are assumed to be in the currency implied by the system locale. To set this property, see Currency system properties.

**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 user locale, stored in the sys_locale table, is determined by the following, in order of consideration.

- User record in which both 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 are always shown in the session currency and are formatted in the Java-specified format for the user locale.

Session and reference currency

The system uses two kinds of currency, session and reference.

The session currency is defined for the user by the user’s locale or single-currency mode. The reference currency is determined by the system locale. The reference currency is a standard used...
across the entire instance. Each time a value is entered in a currency or price field, the system stores three pieces of information:

- The value as entered, in the user’s locale.
- The currency code, in the user’s locale.
- The value converted to the reference currency using the current exchange rate.

**Note:** In multiple-currency mode, the currency code saved in 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
- The 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 session currency is determined by the following, in order of consideration:

- Single-currency mode setup using `glide.i18n.single_currency` and `glide.i18n.single_currency.code`.
- The default currency for the user’s locale.

**Reference currency**

In order to perform calculations on heterogeneous currency values, the platform stores currency values converted to a system currency, referred to as the reference currency. Every currency field in the system contains a reference currency value. The reference currency is determined by the following, in order of consideration:

- The system locale set using the property `glide.system.locale`
- The Java default locale, typically `en_US`

The filtering and aggregation features use the reference currency value to perform calculations on default currency fields. This 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 because the reference currency values are used for filtering but session currency values are displayed.
- Aggregation of currency fields might not produce the expected results because reference currency values are aggregated and then converted to the session currency.
- Currency values might not be formatted as expected because currency values are formatted based on the user’s locale and not on the currency code.

The confusion is caused by 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:

- Single-currency mode changes the currency in the user views and 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.

The effects of rate conversions can be avoided 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.

The conversion and display selections can be chosen per price field and can be changed at any time. There are three variations:

- Calculated (Default): Behaves the same as the default currency field type. Whenever conversions are performed, the latest currency conversion rates are used. When the price field is displayed, it is shown in the user’s session currency.
- Fixed: When the price field is displayed, it is shown in the currency code used when the value was entered. Whenever conversions are performed, the latest currency conversion rates are used.
- Multiple: Enables you to enter multiple price values for an item using a different currency for each price. The field’s value is the value entered in the user’s session currency; otherwise, the first price entered is converted to the user’s session currency. Whenever conversions are performed...
performed, the latest currency rates are used. 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.

A price field’s currency code and numeric value can be changed in a form. An edit icon is shown next to the price field. Clicking the edit icon displays a form that can be used to edit all details of the price field:

- **Currency**: List of currencies enabled in the system in the combo box. In single currency mode, the currency is a label and cannot be changed.
- **Amount**: Numeric value formatted in the user’s locale
- **Type**: Combo box with calculated, fixed, multiple
  - When the price type is changed to multiple, the system creates child records for all currencies enabled in the platform populated with values converted from the amount field using latest currency conversion rates.
  - In single currency mode, the type cannot be changed.
  - The price type can be modified any time.

### Currency values in lists

In lists, currency values are displayed in the user’s session currency formatted for display in the user’s locale. Typically the currency symbol is followed by a formatted number.

Different field types appear as follows:

- **Currency field type**: Value in user’s session currency
- **Price field type/Calculated**: Value in user’s session currency
- **Price field type/Fixed**: Value in currency as entered by the user
- **Price field type/Multiple**: Value associated with the user’s session currency if this value exists; otherwise, the first value entered is converted to the user’s session currency

A Globe icon is displayed beside the currency value that enables the value to be changed 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 are shown as entered, formatted for display in 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:** Because the conversion rate between the currency field’s value (what is displayed) and its reference currency value (used for the aggregation) might have changed, the result may not be what the user expects.

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 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:** Because the conversion rate used when the filter is run might be different than the conversion rate used when calculating the reference values in the individual records, filtering results might not provide the expected result.

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.

**Currency values in forms**

In forms, currency values are shown in the currency in which they were entered.

A combo box gives the list of currencies available in the system. The format is determined by the user’s locale. When entering or changing the numeric value, format the value in the format specified by the user’s locale. In the form for a new record, the combo box with the list of currencies has the reference currency selected, and the numeric value set to zero.

![Currency Field](image)

If the record is read only, the currency value is shown as entered and formatted for display in the user’s locale. A price field shows the session currency value.

In single currency mode, the currency is a label and cannot be changed. The form for editing the details of fields previously mentioned cannot be accessed because the edit icon is not shown.
Editing the currency instance table

For users who can edit the currency instance table (fx_currency_instance), an edit icon appears next to the field. Users with the financial_mgmt_user role can edit the values associated with the currency field.

**Note:** Do not edit the fx_currency_instance table directly. The platform maintains these tables, and your changes could have unintended consequences.

Currency values in reports

Currency values in reports are in the user’s session currency 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.

Currency conversions

Currency values can be converted to other currencies when stored and accessed.

Conversions can happen in these situations.

- The currency value is converted to reference currency when stored, whether on insert or update. This means that the reference currency value is saved as well as the currency value.
- The currency value is converted to the user’s session currency for display.
- The value entered for a filter from currency specified in the filter is converted to the reference currency.

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

- Rate to convert from the first currency to Euro
- Rate to convert from Euro to the second currency

Whenever a conversion is performed, the platform 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. Aggregation therefore 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 ECB Exchange Rate Load to perform a nightly download of currency-conversion tables from the European Central Bank. For information about turning off the regularly scheduled update and maintaining the Exchange Rate table manually, see [Use your own currency-conversion rates](#).

You can adjust the frequency of this behavior or disable it entirely.

1. Navigate to System Scheduler > Scheduled Jobs.
2. Open the job named ECB Exchange Rate Load.
3. Modify the schedule, as needed.

   After the job runs, rates are stored in and loaded 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:


If ECB does not supply the daily rates for a specific currency, you can enter rates manually into the Exchange Rate table, use an import set, or use 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.

---

**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: this 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 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.

**Currency values in scripts**

You can use currency fields in scripts.

These methods are available on GlideElement objects.

To display currency values, use the display APIs `getDisplayValue()`. To work with currency values in any way other than display, use the APIs that return/accept unformatted numbers.

**Note:** Do not use the `getDisplayValue()` methods and then process the string to remove formatting information before performing calculations on the value.

Methods such as `getValue()` and `getCurrencyValue()` return unformatted numbers as strings. The floating point value can be obtained by using the JavaScript function `parseFloat()`. The resulting value can be used to perform calculations. The currency associated with these values can be obtained by 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 the currency is the user's session currency, use a plain number (either 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);
```

When you use GlideAggregate on currency or price fields, you are working with the reference currency value. Be sure to convert the aggregate values to the user's session currency for display. Because the conversion rate between the currency or price field's value (what is displayed) and its reference currency value (used for the aggregation) might have changed, the result may not be what the user expects.

When a record containing a currency value is deleted, 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. See Change currency decimal places for how to change the number of decimal places used by the system. When set 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. This 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.

In the following table, the example values use a currency value of 21345.67 in Japanese yen (1563.72 in Euros and 1152.48 in US dollars) with the user’s locale set to German (de.DE) and reference currency set to USD.

### 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 an 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></td>
<td><strong>Note:</strong> This might not be the session or reference currency.</td>
<td></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>
</tbody>
</table>
### Configure 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>The value entered in the audit record is the numeric value in the session currency. The currency code is not included. This value is the pre-Istanbul behavior and the default.</td>
</tr>
<tr>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>true</td>
<td>The value as entered by the user in the format USD;1234.56.</td>
</tr>
</tbody>
</table>

**Change 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 pre-Istanbul behavior and the default.</td>
</tr>
<tr>
<td>true</td>
<td>Uses four decimal places.</td>
</tr>
</tbody>
</table>

**Configure 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>The optimizer is not used.</td>
</tr>
<tr>
<td>true</td>
<td>The 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.

**Currency system properties**

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 currency fields

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.sys.audit_currency_value</td>
<td>When <strong>true</strong>, currency fields in audit records are the value entered by the user, in the format <strong>USD; 1234.56</strong>. When <strong>false</strong>, the value is the numeric value in the session currency.</td>
</tr>
<tr>
<td><strong>Type</strong>: Boolean</td>
<td><strong>Default value</strong>: false</td>
</tr>
<tr>
<td><strong>Location</strong>: System Property (sys_properties) table</td>
<td><strong>Learn more</strong>: <a href="#">Configure currency fields in audit records</a></td>
</tr>
<tr>
<td>glide.currency_price.use_all_fraction_digits</td>
<td>When <strong>true</strong>, currency fields have four decimal places. When <strong>false</strong>, two decimal places are used.</td>
</tr>
<tr>
<td><strong>Type</strong>: Boolean</td>
<td><strong>Default value</strong>: false</td>
</tr>
<tr>
<td><strong>Location</strong>: System Property (sys_properties) table</td>
<td><strong>Learn more</strong>: <a href="#">Change currency decimal places</a></td>
</tr>
<tr>
<td>glide.currency_price_optimizer.enabled</td>
<td>When <strong>true</strong>, the optimizer is used. When <strong>false</strong>, the optimizer is not used.</td>
</tr>
<tr>
<td><strong>Type</strong>: Boolean</td>
<td><strong>Default value</strong>: true</td>
</tr>
<tr>
<td><strong>Location</strong>: System Property (sys_properties) table</td>
<td><strong>Learn more</strong>: <a href="#">Configure currency optimizer</a></td>
</tr>
<tr>
<td>glide.currency_price_optimizer.min_rows</td>
<td>The 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><strong>Type</strong>: Number</td>
<td><strong>Default value</strong>: 4</td>
</tr>
<tr>
<td><strong>Location</strong>: System Property (sys_properties) table</td>
<td><strong>Learn more</strong>: <a href="#">Configure currency optimizer</a></td>
</tr>
<tr>
<td>glide.excel.convert_to_user_currency</td>
<td>When <strong>true</strong>, currency fields in a table are output in the user's session currency.</td>
</tr>
<tr>
<td><strong>Type</strong>: Boolean</td>
<td><strong>Default value</strong>: false</td>
</tr>
<tr>
<td><strong>Location</strong>: System Property (sys_properties) table</td>
<td><strong>Learn more</strong>: <a href="#">Exporting currency fields to Excel</a></td>
</tr>
</tbody>
</table>
### Property Description

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>glide.excel.fixed_currency_usd</strong></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: <strong>false</strong></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><strong>glide.system.locale</strong></td>
<td>The value is of the format <code>Language.Country</code> 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 <a href="#">Java supported locales</a> 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: <a href="#">Locale settings</a></td>
</tr>
</tbody>
</table>

### Localization settings

Localization settings control translation, currency, and locale settings in the instance.

**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).

### Common locales

<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**.

### Internationalization support

ServiceNow supports multiple languages, using UTF-8 for international characters.

When a user logs in, the system uses either the system default language or the language specified in the user record. This setting determines the language in which forms and messages are displayed throughout the session.

### Language internationalization support

The ServiceNow system supports multiple languages, using UTF-8 for international characters.

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 user’s 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 journal fields, report titles, and any field that stores free-form text. These fields remain in the language used to create them.

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 my custom fields be translated?</td>
<td>When you create a field, it does not create a translated label. Labels for custom fields are created with a language of English (en). You can, however, translate the fields manually.</td>
</tr>
<tr>
<td>Question</td>
<td>Answer</td>
</tr>
<tr>
<td>----------</td>
<td>--------</td>
</tr>
<tr>
<td>I am not seeing journal fields translated.</td>
<td>User-defined string fields, such as short description, additional comments, and report titles are not translated. They appear in the language they were created in.</td>
</tr>
</tbody>
</table>

**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 see if a language is not specified in their user record.

![Default language for the system (two character values):](image)

**User specific language**

The user has several choices for identifying the language to be used for the instance, as described here.

- **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

**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]

**Note:** The Languages table is available only after I18N:Internationalization 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 / Field [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.
Message table
The Message (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:

- **Application**: name of the application this message appears in.
- **Key**: internal unique identifier of this message.
- **Language**: language the message is translated into.
- **Message**: translated text that users see.
Field Label table

The Field Label 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.
- **URL target** (Supported on UI14 and earlier): location where the URL appears, if a URL is given. If this field is empty, the URL opens in the current tab or window when a user clicks the help icon. If the field contains the code _blank, the URL opens in a new tab or window when a user clicks the help icon.
Field label

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>Table</th>
<th>Element</th>
<th>Language</th>
<th>Value</th>
<th>Dependent value</th>
<th>Label</th>
<th>Inactive</th>
<th>Sequence</th>
<th>Hint</th>
</tr>
</thead>
<tbody>
<tr>
<td>task</td>
<td>approval</td>
<td>en</td>
<td>not requested</td>
<td>Not Yet Requested</td>
<td>false</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>task</td>
<td>approval</td>
<td>fr</td>
<td>not requested</td>
<td>Pas encore demandé</td>
<td>false</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>task</td>
<td>approval</td>
<td>fr</td>
<td>requested</td>
<td>Demandé</td>
<td>false</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>task</td>
<td>approval</td>
<td>en</td>
<td>requested</td>
<td>Requested</td>
<td>false</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>task</td>
<td>approval</td>
<td>fr</td>
<td>approved</td>
<td>Approuvé</td>
<td>false</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>task</td>
<td>approval</td>
<td>fr</td>
<td>rejected</td>
<td>Réfusé</td>
<td>false</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>task</td>
<td>approval</td>
<td>en</td>
<td>rejected</td>
<td>Rejected</td>
<td>false</td>
<td>3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Translated choice list

#### Translated text

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.
When setting up translations for the different areas of your instance, a property can be turned on that allows you to easily determine which table you need to add the translated label to.

Role required: admin

1. Navigate to System Properties > System Localization.
2. Select Display translation prefix on translatable strings.
3. After activating the property, refresh your browser.
4. Following the refresh, the following prefixes appear on fields, labels, and messages that have been translated internally.
Translate new customizations

When using one of the Internationalization plugins, most of the fields in the instance are automatically translated. However, customizations are not translated automatically, and need to be translated by hand. In this case, it is best to locate the individual untranslated strings, and insert those translations manually.

Below are three tools for locating untranslated strings:

- Displaying prefixes for translatable strings
- Exporting untranslated strings
- Using the translate and learn property

Locate translatable strings

These tables contain translatable strings, described more at length in Language Internationalization.

- Translated Name / Field (sys_translated)
- Message (sys_ui_message)
- Field Label (sys_documentation)
- Choice (sys_choice)

Display a translation prefix

Translation prefixes indicate where to find the string for translation.

Role required: admin

1. To enable prefixes on field labels for the current user session, navigate to System Localization > Enable I18N Debugging.
2. To disable prefixes for the current session, navigate to System Localization > Disable I18N Debugging.
For the prefix TRF, navigate to System Localization > Translated Names / Fields.
For the prefix MSG, navigate to System Localization > Messages.
For the prefix GMLD, navigate to System Localization > Field Labels.
For the prefix TRT, navigate to System Localization > Translated Text.
For the prefix CHC, navigate to System Localization > Choices.

Some few strings may not display translatable prefixes. This means that the string is not stored on any of these four tables. This behavior occurs with text embedded in images, such as the buttons in the Service Catalog, or text defined by properties, such as the text which follows the banner.

You must refresh your browser after accessing one of these modules to apply the change.

Export an untranslated string
One method for easily translating customizations is to export all of the translated names and fields, messages, field labels, and choices that only have English translations.

Role required: admin
To aid in this, there are four modules for the System Localization application menu that are active by default.

- Translated Name / Fields
- Messages
- Field Labels
- Choices

Note: The Customizations module is inactive by default. You must activate it to make it visible on the System Localization application menu.

1. Perform the appropriate action for your version of the UI:

   | UI16 | 1. Navigate to System Definition > Application Menus  
   |      | 2. Select System Localization. |
   | UI15 or UI11 | Right-click the System Localization application menu and select Edit Application Menu. |

2. Use the list editor to set the Active field to True for the modules.
After the application navigator refreshes, the modules appear. Now it is possible to export the list of untranslated fields by viewing each of the lists and exporting it to any supported format. **Use the translate and learn property**

The `glide.translate.learn` system property, when set to true, creates records in the translate tables when an instance encounters text that should be translated, but no corresponding record exists. You can use this property to help locate untranslated strings.

**Note:** Using this method hampers the use of the exporting untranslated strings method.

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:

![HR application missing translations](image)

The suffix (fr) indicates that there is a French translation missing. Because translation prefixes are enabled, the prefix **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):

![Example untranslated modules](image)

**Service catalog buttons**

You can specify language-specific messages for buttons in these service catalog screens: Cart, Edit Cart, and Check Out (including workflows and approvals).
The text for the buttons is stored on the "Messages" table.

Activate a language

By default, the language supported by the platform is American English. You can activate 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 (deprecated)
- I18N: Polish Translations
- I18N: Portuguese Translations
- I18N: Russian Translations
- I18N: Simplified Chinese Translations
- I18N: Spanish 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 an instance.

Note: Activating internationalization plugins for any of the available languages automatically activates the I18N: Knowledge Management Internationalization Plugin v2 plugin (com.glideapp.knowledge.i18n2).

Use the following steps to activate the desired language plugins.

1. Navigate to System Definition > Plugins.
2. Find and click the plugin name.
3. On the System Plugin form, review the plugin details and then click the Activate/Upgrade related link.
   - If the plugin depends on other plugins, these plugins are listed along with their activation status.
   - If the plugin has optional features that depend on other plugins, those plugins are listed under Some files will not be loaded because these plugins are inactive. The optional features are not installed until the listed plugins are installed (before or after the installation of the current plugin).
4. Optional: If available, 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 practice when you first activate the plugin on a development or test instance.
   - You can also load demo data after the plugin is activated by clicking the Load Demo Data Only related link on the System Plugin form.
5. Click Activate.

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 for more information.

See Price fields for information on the types of price fields supported.
See Currency values in scripts for information on using currency fields in scripts.

Use translated text

Each instance can be localized, translating the instance to the instance’s local language.

Translated text fields allow the same field to display different content based on the user’s language.

There are two different translated text fields:
These fields operate the same as text and HTML fields respectively, except that they can store multiple inputs in multiple languages.

The most frequent uses of translated text fields are in the Knowledge Base (e.g. article titles or content) or the Service Catalog (e.g. names, descriptions, or variables). The Knowledge Base also has an option for internationalization with the Knowledge Management Internationalization Plugin, which allows for language-specific articles rather than translating articles.

**Note:** The type is translated separately from Translated Text and Translated HTML fields.

### Administer 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 master table, but the values of other are stored in the `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.

Key Fields in the Translated Text [sys_translated_text] Table:

- `tablename` -- the table to which this translation belongs, e.g., problem
- `fieldname` -- the field to which this translation belongs, e.g., workaround
- `documentkey` -- the sys_id of the row to which this translation belongs, e.g., the sys_id of PRB00008
- `language` -- the two character ISO language code to which this translation belongs

### Use translated text

Each instance can be localized, translating the instance to the instance's local language.

Translated text fields allow the same field to display different content based on the user's language.

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 uses of translated text fields are in the Knowledge Base (e.g. article titles or content) or the Service Catalog (e.g. names, descriptions, or variables). The Knowledge Base also has an option for internationalization with the Knowledge Management Internationalization Plugin, which allows for language-specific articles rather than translating articles.

**Note:** The type is translated separately from Translated Text and Translated HTML fields.

### Translate the content of a translated text field

After a translated text field or translated HTML field has been created and is in use, it displays English when viewed in a different language until the content is translated.
Be sure to confirm that the field is in fact a translated text field, and not a regular text or HTML field, for example, by right-clicking the field and choosing Personalize Dictionary.

The method below works best for one-off translations. To translate large numbers of translated text fields, use the Exporting Untranslated Strings method.

1. Use the language picker to switch to the language the field’s content is being translated to.
2. Navigate to the field on the form.
3. Replace the English text with the text of the target language.
4. Submit.

Now the text will display English when the user’s language is English and in the new language when the user’s language is set to that new language.

System localization

Localization allows administrators to accommodate users from a variety of different countries, using different languages and currencies, within the same instance.

The platform supports internationalization of language and localization of currencies and prices wherever they appear.

Set 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.

1. Navigate to System Properties > System Localization.
2. Set these properties

<table>
<thead>
<tr>
<th>Customization properties for system localization</th>
<th></th>
</tr>
</thead>
</table>
| **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.** glide.ui.login.language.select | **Enables language selection upon login.**
| | **Options:** Yes | No
| | **Default value:** Yes
| | **Dependency:** The I18N: Internationalization plugin must be active |
| **Text Search stemming language.** glide.ts.stemming_language | **Selects the language to match derived words in text search.**
| | **Options:** English, German, and French
| | **Default value:** English
| | **Dependency:** The I18N: Internationalization plugin must be active
<p>| | <strong>Learn more:</strong> Zing matches derived words with stemming |</p>
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays translation prefix on translatable strings.</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>Options: Yes</td>
</tr>
<tr>
<td></td>
<td>Default value: No</td>
</tr>
<tr>
<td></td>
<td>Learn more: Display a translation prefix</td>
</tr>
<tr>
<td>Use a single currency model. Display all currencies in the same currency code, regardless of a user’s locale, country, or language code.</td>
<td>Enable single currency mode.</td>
</tr>
<tr>
<td>glide.i18n.single_currency</td>
<td>Options: Yes</td>
</tr>
<tr>
<td></td>
<td>Default value: No</td>
</tr>
<tr>
<td></td>
<td>Learn more: Currency administration</td>
</tr>
<tr>
<td>Default language for the system (two character values)</td>
<td>Options: en, fr, es, it, de</td>
</tr>
<tr>
<td>glide.sys.language</td>
<td>Default value: en</td>
</tr>
<tr>
<td></td>
<td>Learn more: Display a translation prefix</td>
</tr>
<tr>
<td>If using the single currency model, display all currencies using this currency code.</td>
<td>Options: ISO 4217 three-letter currency code</td>
</tr>
<tr>
<td>Currency codes use the ISO 4217 three letter format.</td>
<td>Default value: USD</td>
</tr>
<tr>
<td>glide.i18n.single_currency.code</td>
<td>Learn more: Currency administration</td>
</tr>
<tr>
<td>Locale code to use for localization.</td>
<td>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.</td>
</tr>
<tr>
<td>glide.system.locale</td>
<td>Options: (language code).(country code) (for example, en.GB for Britain, fr.FR for France, de.DE for Germany, or ja.JP for Japan)</td>
</tr>
<tr>
<td></td>
<td>Default value: None</td>
</tr>
<tr>
<td></td>
<td>Learn more: Locale settings</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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.</td>
</tr>
<tr>
<td>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).</td>
<td>Adds the current language suffix to UI elements such as labels and messages. Enabling the language suffix assists with translating new customizations.</td>
</tr>
<tr>
<td>glide.translate.learn</td>
<td>Options: Yes</td>
</tr>
<tr>
<td></td>
<td>Default value: No</td>
</tr>
<tr>
<td></td>
<td>Dependency: The I18N: Internationalization plugin must be active</td>
</tr>
<tr>
<td></td>
<td>Learn more: Use the translate and learn property</td>
</tr>
</tbody>
</table>
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.

Translate an instance

ServiceNow provides a series of Internationalization plugins, each of which translates most of the instance into a particular language.

Administrators can also translate an instance into languages other than those provided in the internationalization plugins. For a list of available languages, see Activate a language.

Activate the I18N: Internationalization plugin

The first step in translating an instance is to install the elements required for translation, including tables to hold the translations, language pickers to allow users to switch between languages, and import set tables and transform maps to aid in importing translations. These elements are all provided in the plugin I18N: Internationalization.

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: Enter sys_user.
   - Element: Enter preferred_language.
   - Language: Enter the two-character ISO 639.1 code for the language this choice record is a member of. For example, tr. The default is en.
   - Label: Enter the name of the language selection as you want it to appear in the language picker. For example, Turkish.
• Value: Enter the two-character ISO 639.1 code for the new language selection. For example, tr. The instance uses this value to set the display language.
• Sequence: 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.

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.

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.
   \begin{itemize}
     \item For choices, select the Sys Choice Translation Map.
   \end{itemize}

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 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 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:

```javascript
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 **Translate the Interface**.

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.

4. Click Submit.

   This creates a new record in the Translated Name / Field table for the selected language or updates the existing record.

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.

**Translate long text content**

Long text content occurs in fields with the type translated_text or translated_html.

Use the following procedure to translate the content for individual text fields. To translate large numbers of text or HTML fields, use the procedure described under Translate the Interface.

To translate the content of a text or HTML field on a form (field type translated_text or translated_html):

1. Use the language picker to switch to the desired language.
2. Navigate to the field on the form.
3. Replace the English text with the text of the target language.
4. Click Submit.

   This creates a new record in the Translated Text table for the active language. The field content displays English or the new language, depending on the user's language selection.

**Translate the interface**

After creating the choice record, translate the interface, including the applications, modules, UI actions, forms, lists, alerts, and choice lists.

All of these interface items are stored as translatable strings in these translation tables:

- Translated Name / Field [sys_translated]
- Messages [sys_ui_message]
- Field Label [sys_documentation]
- Choice [sys_choice]
- Translated Text [sys_translated_text]

By default, these translation tables only contain English strings. To populate these tables with translated strings:

1. Export the contents of the translation tables into a format (such as Excel) that can be easily manipulated.
2. Within the exported document, translate the Label, Plural, Hint, and Message columns for each row. Be sure to also change the "Language" column to the two character ISO code of the new language.
3. Import the translated document back into the instance as an import set.
### Self-localize the interface

If self-localizing the base system (for languages not supported by ServiceNow or deprecated), ServiceNow provides a file containing strings from the interface in the English language. This file can be translated into any language and imported to the instance.

All interface items are stored as translatable strings in these translation tables:

- Translated Name / Field [sys_translated]
- Messages [sys_ui_message]
- Field Label [sys_documentation]
- Choice [sys_choice]
- Translated Text [sys_translated_text]

By default, these translation tables only contain English strings. To populate these tables with translated strings:

1. Obtain the file containing English strings from the translation tables. This file is provided by ServiceNow.
2. Within the file, translate the Label, Plural, Hint, and Message columns for each row. Be sure to also change the “Language” column to the two character ISO code of the new language.
3. Import the translated document back into the instance as an import set.

### 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 Translate the Interface.

**Note:** In addition to translated field types, currency fields display the same price in different currencies based on the user's language.

### Translate the knowledge base

The knowledge base has two separate methods for translation.
Translating the content of articles: used for articles that apply to users of all languages.
Creating language-specific articles: used when users with different languages need different articles.

Translating knowledge base articles

Knowledge base articles use translated_html fields for article content. This type of field displays the translation based on the user's language, if multiple translations are stored. To learn about using translated_html fields, see Use Translated Text.

Creating language-specific articles

Activating the Knowledge Management Internationalization v2 plugin adds a Language field on the Knowledge form for setting the language of the article. Users can choose a language to search and search results return only articles in that language. Users can switch between different translations of the same article, as well.

Time configuration

Time configuration involves the scheduling of events and tracking of time across applications.

Date and time fields

Records can store date and time values in several different types of fields. These values are stored in the database as integer numbers of milliseconds, and are displayed in the appropriate date or time format.

Date and time field types

The following field types are provided for storing date and time information in records.

<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 list 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 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 anything other than three characters, an Invalid Date appears error appears when you attempt to 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’.

You should also note that 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 to use a yyyy format-based date. For example, 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. Note that 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 to use a yyyy format-based date. For example, 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>The date picker displays a calendar as well as a field for manual date entry.</td>
</tr>
<tr>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>true</td>
<td>The date picker displays a calendar only. This is the default behavior in UI16 and UI15.</td>
</tr>
</tbody>
</table>
Default date and time fields

Certain time fields are provided by default to store particular date and time fields.

Global timestamp fields

All records inherit certain time stamp fields from the Global (global) table.

- Created
- Updated

These fields are automatically populated with the correct date and time.

Planned Task time fields

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.

Task fields for measuring work time

Use default task fields to measure progress and resolution for certain records.

The following base system fields are provided on certain tables to keep track of how long it takes to close tickets:

- **Time worked**: A timer which runs while the record is being viewed by a user, and pauses while the record is closed (or when it is paused manually). Used to keep track of the time spent by the help desk while working on the record.
- **Resolve time**: A calculated field which measures the time from the moment the record is opened, to the moment the record is closed. Used to keep track of how long it takes to resolve the record.

These fields provide different metrics for request response.

The following additional tools are available for tracking work time:

- **Service level agreements (SLAs)**: measure how long it takes a record 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)

**Time worked field**

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 (task_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.

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 field when the record is resolved or marked closed, and measure the difference between the Opened and Closed dates.

On the Incident table, the field is calculated on incident resolution, or closure, whichever happens first, based on the business rule `mark_resolved` or `mark_closed`. Both are based on Incident table get trigger.

When the incident is resolved, the calculation is based on the `mark_resolved` business rule. 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 number of seconds.

1. From the Incident or Request form, right-click the form header and click Configure > Table. The system displays the table form.
2. From the Columns embedded list, click Resolve time. The system displays the dictionary entry for the field.
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.
Forms and lists display the resolve time as a number of days, hours, and minutes. 

**Note:** This attribute does not change the field data format which remains an integer representing a number of seconds. Reports and data exports will still display the actual number of seconds rather than a duration.

### Export date and time formats

Because some export formats are intended for human consumption and others are intended for database usage, different methods provide date and time field information in different formats.

#### Excel

Date, Date-Time, and Time fields are all exported as their display values, displayed using a custom format instead of the system date format. Duration fields, however, 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} setting in System Properties, and you export time values to Excel, they show in 24-hour military time format. To display the exported values in standard 12-hour am/pm time formats, select the \texttt{1:30PM} time format in \texttt{Format Cells \> Time} in Excel.

\texttt{hh:mm:ss}

#### 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.

### Calendars and schedules

Specific applications within the platform generate graphical calendar displays based on Schedule Pages. These Schedule Pages can be displayed in a daily, weekly, or monthly view. 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, most instances should 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.

Calendar content is controlled by a Schedule Page (cmn_schedule_page) record. To access Schedule Pages, navigate to System Scheduler > Schedules > Schedule Pages. The Schedule Pages form provides the following fields:

The Schedule Page record contains 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 identify the current schedule page.</td>
</tr>
<tr>
<td>Schedule type</td>
<td>String</td>
<td>The 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: $/show_schedule_page.do?sysparm_page_schedule_type=gantt_chart&amp;sysparm_timeline_task_id=d530bf907f0000015ce594fd929cf6a4$ Alternatively, the schedule page can also be accessed by setting the 'sysparm_page_sys_id' URI parameter to that of the unique 32 character hexadecimal system identifier of the schedule page.</td>
</tr>
</tbody>
</table>
| 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. Note: This functionality is only used by Calendar type schedule pages. |

© 2019 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 Type Table

<table>
<thead>
<tr>
<th>Field</th>
<th>Field Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTML</td>
<td>String</td>
<td>The HTML field is a scriptable section that is parsed by Jelly and injected 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 and is discussed below.</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 to be displayed.</td>
</tr>
</tbody>
</table>

### Calendar views from the schedule pages

A "URL from arguments" module, a field decoration (dictionary attribute "ref_contributions"), or a UI Action linking to "show_schedule.do" is used 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,
```

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 will default 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, it will display only the valid views. If all values are invalid, the default three views will be displayed and will rewrite 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 will filter by the specified group. Valid value is a group sysId.

© 2019 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 URL component `sysparm_start_date=2016-03-02` determines the date based on which every view is displayed. If `sysparm_start_date` is specified, it will open the calendar displaying 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.

### Fiscal calendars

With fiscal calendars you can define fiscal periods, such as one month long or four weeks long or Q1 2015 or July 2015.

To create a fiscal calendar, activate the Fiscal Calendar (com.snc.fiscal_calendar) plugin.

**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.

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></td>
<td><strong>Note:</strong> This calendar is the only type that does not use quarters.</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>
<tr>
<td>454</td>
<td>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.</td>
</tr>
<tr>
<td>544</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Activate the Fiscal Calendar

You can activate the Fiscal Calendar plugin (com.snc.fiscal_calendar) if you have the admin role.

Role required: admin

1. Navigate to **System Definition > Plugins**.
2. Find and click the plugin name.
3. On the System Plugin form, review the plugin details and then click the **Activate/Upgrade** related link.

   If the plugin depends on other plugins, these plugins are listed along with their activation status.

   If the plugin has optional features that depend on other plugins, those plugins are listed under **Some files will not be loaded because these plugins are inactive**. The optional features are not installed until the listed plugins are installed (before or after the installation of the current plugin).

4. Optional: If available, 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 practice when you first activate the plugin on a development or test instance.

   You can also load demo data after the plugin is activated by clicking the **Load Demo Data Only** related link on the System Plugin form.

5. Click **Activate**.

---

**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.

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.
### Field

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fiscal Calendar Types</td>
<td>Select the type of calendar by clicking it. The options in the choice lists update automatically.</td>
</tr>
</tbody>
</table>
| Fiscal Unit            | Select the base unit for the calendar:  
                          - **Month**: Generate fiscal calendar with monthly periods.  
                          - **Quarter**: Generate fiscal calendar with quarterly periods. |
| Start Month            | Select the month that is the beginning of your fiscal year.                  |
| Start Year             | Select the year.                                                             |
| Prefix for Year        | Enter a prefix that the application uses in the name of the records that represent the fiscal year. |
Field | Description
--- | ---
Prefix for Quarter/Period | Enter a prefix that the application uses in the name of the records that represent the fiscal quarter or period.
Start Day | Select the day that represents the beginning of each month.
End Year | Select the year the calendar ends.
Prefix for Month/Period | Enter a prefix that the application uses in the name of the records that represent the month or period.

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.

Fiscal period form fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the fiscal period.</td>
</tr>
<tr>
<td>Start date time</td>
<td>The date the fiscal period starts.</td>
</tr>
<tr>
<td>End date time</td>
<td>The date the fiscal period ends.</td>
</tr>
<tr>
<td>Fiscal Type</td>
<td>(Read-Only) The type of period, either <strong>Year</strong> or <strong>Quarter</strong>.</td>
</tr>
</tbody>
</table>

3. Validate the fiscal periods to ensure 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**.

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.

Default schedules

Default schedules are available in a base system.
### Default Schedules

<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>Name</td>
<td>Schedule</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>--------------------------------------------------------------------------</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**

Each individual holiday can be defined 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 to ensure that 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

**Name:** U.S. Holidays

**Time zone:** [Floating]

**Description:**
Sample set of holidays recognized in the United States

### Related Links

#### Show Schedule

**Schedule Entries (12)**

<table>
<thead>
<tr>
<th>Schedule Entries</th>
<th>Child Schedules</th>
<th>Referenced By (1)</th>
</tr>
</thead>
</table>

#### Schedule Entries

<table>
<thead>
<tr>
<th>Name</th>
<th>Repeats</th>
<th>Repeat every</th>
<th>Start date time</th>
<th>End date time</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Christmas Day</td>
<td>Every year on Dec 25</td>
<td>1</td>
<td>12-25-2012 00:00:00</td>
<td>12-25-2012 23:59:59</td>
<td>Excluded</td>
</tr>
<tr>
<td>Christmas Eve</td>
<td>Ever year on Dec 24</td>
<td>1</td>
<td>12-24-2012 00:00:00</td>
<td>12-24-2012 23:59:59</td>
<td>Excluded</td>
</tr>
<tr>
<td>Columbus Day</td>
<td>Every year on 2nd Mon of Oct</td>
<td>1</td>
<td>10-09-2012 00:00:00</td>
<td>10-09-2012 23:59:59</td>
<td>Excluded</td>
</tr>
<tr>
<td>Independence Day</td>
<td>Every year on July 4</td>
<td>1</td>
<td>07-04-2012 00:00:00</td>
<td>07-04-2012 23:59:59</td>
<td>Excluded</td>
</tr>
<tr>
<td>Labor Day</td>
<td>Every year on 1st Mon of Sep</td>
<td>1</td>
<td>09-01-2012 00:00:00</td>
<td>09-01-2012 23:59:59</td>
<td>Excluded</td>
</tr>
<tr>
<td>Martin Luther King, Jr. Day</td>
<td>Every year on 3rd Mon of Jan</td>
<td>1</td>
<td>01-16-2012 00:00:00</td>
<td>01-16-2012 23:59:59</td>
<td>Excluded</td>
</tr>
<tr>
<td>Memorial Day</td>
<td>Every year on last Mon of May</td>
<td>1</td>
<td>05-28-2012 00:00:00</td>
<td>05-28-2012 23:59:59</td>
<td>Excluded</td>
</tr>
<tr>
<td>New Year's Day</td>
<td>Every year on Jan 1</td>
<td>1</td>
<td>01-01-2012 00:00:00</td>
<td>01-01-2012 23:59:59</td>
<td>Excluded</td>
</tr>
<tr>
<td>New Year's Eve</td>
<td>Every year on Dec 31</td>
<td>1</td>
<td>12-31-2012 00:00:00</td>
<td>12-31-2012 23:59:59</td>
<td>Excluded</td>
</tr>
<tr>
<td>Presidents' Day</td>
<td>Every year on 3rd Mon of Feb</td>
<td>1</td>
<td>02-20-2012 00:00:00</td>
<td>02-20-2012 23:59:59</td>
<td>Excluded</td>
</tr>
<tr>
<td>Thanksgiving Day</td>
<td>Every year on 4th Thu of Nov</td>
<td>1</td>
<td>11-22-2012 00:00:00</td>
<td>11-22-2012 23:59:59</td>
<td>Excluded</td>
</tr>
<tr>
<td>Veterans Day</td>
<td>Every year on Nov 11</td>
<td>1</td>
<td>11-11-2012 00:00:00</td>
<td>11-11-2012 23:59:59</td>
<td>Excluded</td>
</tr>
</tbody>
</table>
The following example shows a schedule that includes the holiday schedule shown above.

**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 that all follow the same work schedule (for example, an 8-5 weekdays schedule) but have 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 instead make the regional holiday schedule a child schedule of the work hours schedule, you will need to create a separate work hours schedule for each region. The total number of schedules in this case is \(<\text{number of schedules}\times2\) schedules.

### Parent and child schedules

Schedules can have one of two parent-child relationship 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.

Parent schedules are not valid if they are only exclusionary. They must have at least one entry that is not of type **Excluded**.

---

**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.

---

### Schedule entry fields

The **Schedule Entries** related list contains the definitions of the time periods you want to include in or exclude from the schedule.

---

**Note:** A schedule entry can only be associated with one schedule.

---

The Schedule Entry form uses these fields.

<table>
<thead>
<tr>
<th><strong>Schedule Fields</strong></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>Show As</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>When</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Repeats</td>
</tr>
<tr>
<td>Repeat every</td>
</tr>
<tr>
<td>Repeat on</td>
</tr>
<tr>
<td>Field</td>
</tr>
<tr>
<td>---------------</td>
</tr>
</tbody>
</table>
| Monthly type  | Select how a monthly schedule repeats. 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 week day in the last week of the month               |
| Yearly type   | Select how a yearly schedule repeats. 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    | Select which 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     | Select which 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         | Select which 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  | Select a repetition end date. If you leave this field blank, the schedule repeats indefinitely. |
| Type          | (Optional) Enter a schedule entry description.                                |

### Schedule fields

The Schedule form uses these fields.

#### Schedule Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique name for the schedule.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>Select the time zone for the schedule. If you select Floating, the time zone will be relative to whatever is accessing the item at any given time. 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. 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>Select a parent schedule to constrain the new schedule.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Type  | Enter a label that describes the purpose of the schedule. The system also uses the schedule type to determine how to process certain schedules.  
- Excluded: excludes time periods from SLA counts.  
- Maintenance: specifies time periods where change management activities are allowed. A schedule containing maintenance schedule entries cannot also contain blackout schedule entries.  
- Blackout: excludes time periods from change management schedules. A schedule containing blackout schedule entries cannot also contain maintenance schedule entries. |
| Description | Describe the schedule. |

**Define a schedule**

Schedules are configured with two types of 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 \( \text{cmn\_schedule} \) table.
- Schedule entry records specify the time periods that are included or excluded from a schedule. Schedule entries are saved in the Schedule Entry \( \text{cmn\_schedule\_span} \) 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.

**Note**: The Schedule form displays a warning message if there are no active entries defined for the current schedule. If your schedule is a child schedule that only contains exclusions, ignore the message because exclusions are non-active entries.
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Type  | Label that describes the purpose of the schedule. You can also use one of these system terms to determine how to process certain schedules:  
- **excluded**: excludes time periods from SLA counts.  
- **maintenance**: specifies time periods where change management activities are allowed. A schedule containing maintenance schedule entries cannot also contain blackout schedule entries.  
- **blackout**: excludes time periods from change management schedules. A schedule containing blackout schedule entries cannot also contain maintenance schedule 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 value for the **Type** field, view the list of schedules rather than the schedule form and add the **Type** column if necessary. You can double-click the cell for the value in the **Type** column and modify from the list view.

4. Configure one or more schedule entries.
### Schedule

<table>
<thead>
<tr>
<th>Name</th>
<th>8-5 weekdays</th>
</tr>
</thead>
<tbody>
<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>

**Update** | **Delete**

#### Related Links

**Show Schedule**

<table>
<thead>
<tr>
<th>Schedule Entries (1)</th>
<th>Child Schedules</th>
<th>Referenced By</th>
</tr>
</thead>
</table>

#### Schedule Entries

**Schedule = 8-5 weekdays**

- **Name**: Monday-Friday 8-5
- **Repeats**: Weekly on Weekdays
- **Repeat every**: 1
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 is displayed 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, you can click the event and in the Event pop-up window, click **Edit** to modify the required fields.

**Modify event**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Displays the name of the event.</td>
</tr>
<tr>
<td>Type</td>
<td>Displays the type of the event. For example, time off, appointment, meeting.</td>
</tr>
<tr>
<td>Show as</td>
<td>Displays the status that is visible when the event starts.</td>
</tr>
<tr>
<td>When</td>
<td>Displays the date and time when the event starts and ends.</td>
</tr>
<tr>
<td>All day</td>
<td>If selected, the event becomes a continuous event irrespective of the date and time mentioned in the <strong>When</strong> field.</td>
</tr>
<tr>
<td>Repeats</td>
<td>Specifies the value when the event needs to be repeated.</td>
</tr>
<tr>
<td>Repeat until</td>
<td>Specifies the date till 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 the event to be delete from that specific day till 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 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 for schedules**

Domain separation is a way to separate data into (and optionally to separate administration) by logically-defined domains. You must activate the Domain Support (com.glide.domain) plugin to enable the domain separation functionality for schedules.
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:

![Diagram of domain support for schedules]

Custom domain support implementations

When you migrate to the new release (london) with a custom implementation of domain support for schedule related tables such as Schedule Entry (cmn_schedule_span), support for domain separation is not automatically introduced. This is to avoid 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 then the script does not introduce the domain_master attribute to the child table.

For example, considering the relationship of the Schedule (cmn_schedule) (parent) and Schedule Entry (cmn_schedule_span) (child) tables, if the upgrading instance has the Domain (sys_domain) column available on both tables then the utility is required to migrate to the base system implementation of domain support for schedules as it is not migrated automatically. If the script detects that there are records where the child Schedule Entry (cmn_schedule_span) domain differs to its parent Schedule (cmn_schedule) domain then it Stops executing and logs a warning with the same reason. If the script does not find any differing records, it proceeds to deactivate and limit 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 domain between a child and parent record remain the same as the domain for the child is derived from the specified reference field.

---

**Schedule for the fifth instance of a day of the week**

When selecting a date near the end of a month for a repeating monthly schedule, it is possible to select a date that computes to the fifth instance of that week day.

ServiceNow offers three options for handling months that do not have a matching fifth instance of the selected day.

- **Last:** ServiceNow selects the last instance of the week day in the month.
- **Next:** ServiceNow selects the first instance of the week day in the next month.
- **Strict:** ServiceNow skips any month without a matching fifth instance and selects only months that have a matching fifth instance.

The system property **glide.schedules.fifth** controls how a schedule entry that selects the fifth occurrence of a week day behaves in months containing only four occurrences of that day. 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 week day 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 that November 29 is the fifth Thursday in the month)

   ![Calendar Image](image)

6. Click **Submit**.
7. Open the same schedule entry.
   
   Note that the form says "Every month on the fifth Thu."
The schedule for the first three months is computed as:

- November 29, 2012 (5th Thursday of the month)
- December 27, 2012 (Last Thursday of the month)
- January 31, 2013 (5th Thursday of the month)

8. If the Value on the `glide.schedules.fifth` property is set to next instead of last in step 3, the schedule for the first three months is computed as:

- November 29, 2012 (5th Thursday of the month)
- January 3, 2012 (1st Thursday of the next month since December 2012 does not have five Thursdays)
- January 31, 2013 (5th 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 (5th Thursday of the month)
- No meeting (December 2012 skipped because it does not have five Thursdays)
- January 31, 2013 (5th 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.

For monthly schedules (Repeat is set to Monthly) that start on a particular day of the month (Monthly type is set to Day of the month), you can specify the following options:

- How ServiceNow computes the starting day each month.
- How ServiceNow handles monthly schedules that start on the fifth instance of a day.

For more information about these computations, see `Fifth Instance of a Day of the Week`.

Day of the Week:

ServiceNow offers two methods to compute what day of the week a monthly schedule repeats on:

- Day: This method computes the day of the week to repeat on by determining the order of the selected starting date within the month. For example, if the selected starting date appears on the first Monday in the month, the schedule repeats every first Monday of every month.
- Week: This legacy method computes 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.

The system property `glide.schedules.repeat_nth` determines 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.

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 that November 5 is the first Monday in the month, but it is in the second week)

6. Click Submit.
7. Open the Schedule Entry.

   Note that the form says Every month on the first Mon.

   The first few dates this schedule will run are:
   - November 5, 2012 (1st Monday of the month)
   - December 3, 2012 (1st Monday of the month)
   - January 7, 2012 (1st Monday of the month)

8. If the Value on the `glide.schedules.repeat_nth` property is set to `week` instead of `day` in step 3, the first few dates this schedule will run are:
   - November 5, 2012 (Schedule starts on Monday in the 2nd week of the month)
   - December 10, 2012 (2nd Monday in the month)
   - January 14, 2012 (2nd Monday in the month)
Client transaction timings

The Client Transaction Timings plugin enhances the system logs by providing more information on the durations of transactions between the client and the server.

By providing information on how time was spent during the transaction, performance issues can be tracked down to the source by seeing where the time is being consumed.

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 module Client Transactions to the System Logs application, which provides a list of every logged transaction between client and server within the last day. The following information is tracked:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created</td>
<td>The moment the transaction was recorded.</td>
</tr>
<tr>
<td>Response Time</td>
<td>The number of ms spent by the server in fulfilling the transaction.</td>
</tr>
<tr>
<td>Business Rule Time</td>
<td>The number of ms spent by business rules triggered by the transaction.</td>
</tr>
<tr>
<td>SQL Time</td>
<td>The 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>The number of ms spent by the network the client is connecting through.</td>
</tr>
<tr>
<td>Browser Time</td>
<td>The 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>The number of ms spent executing ui policy</td>
</tr>
<tr>
<td>Type</td>
<td>Type of transaction (one of Form, List, Other)</td>
</tr>
<tr>
<td>Table</td>
<td>The table that was displayed e.g. incident, change_request</td>
</tr>
<tr>
<td>View</td>
<td>The 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>The order during the load that this operation occurred</td>
</tr>
<tr>
<td>Type</td>
<td>The 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 particular 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.

Properties

The property `glide.client.track_transaction_timings` enables and disables the plugin.

Scripts

The plugin relies on the new script include AJAXClientTiming. This is the script that gathers the information required and populates them on the syslog_client_transaction table.

Dependencies

This plugin does not require any other plugins, but will not gather information unless the 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.

Disabling the Plugin

Although plugins cannot be removed, the functionality can be disabled:

1. Enter `sys_properties.list` in the application navigator filter.
2. Locate the property named `glide.client.track_transaction_timings`.
3. Set the property value to `false`. 
The functionality can be enabled again by setting the property value to `true`.

**Timing values**

Timing values are broken down into several sections.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>start_time</td>
<td>The date and time the user requests a page (the user clicks on a link). This value is set by hooking into the beforeunload event of the previous page. The beforeunload event is not properly supported by WebKit browsers, which is why the client timings are not supported on Safari or Chrome.</td>
</tr>
<tr>
<td>load_time</td>
<td>The date and time that the current page starts loading in the browser. This value is set by an inline javascript that runs as the first script in the HTML body.</td>
</tr>
<tr>
<td>server_time</td>
<td>The 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>The 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>Calculates the 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>This is the 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>Calculates the time the network takes to process the request 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>Calculates the 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 baseline Relative Durations are available:

- 2 business days by 4pm
- 3 business days by 4pm
- Next business day by 4pm
- End of next business day

**Note:** Business day durations are defined by the business schedule used. If no schedule is defined, the durations are 24 X 7 by default.

We will start by looking 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 we want the result of this calculation to land one day in the future. The rest of the script is as in the screenshot below. If
desired, you can customize the time at which you want the Relative Duration to end (currently set to 5pm).

![Relative Duration](image)

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 we will look at **2 business days by 4pm**.

As you can see in the image below, 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 additional day is added to the calculation. Hence the description of **2 business days by 4pm if before 10am**.

![Relative Duration](image)

Note that “End of the business day” has nothing to do with the associated Schedule. The end time of 17:00 is hardcoded into this Relative Duration script. If you want the time to be different than the out of the box 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 to select to calculate either 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 below, also setting a Schedule and a Timezone if you want.

![SLA settings](image)

3. To show how this Relative Duration works, create a new incident.

Notice that the SLA is started for this incident. If you look at the **Planned End Date** field you will notice that the date is the next business day at 5pm (See image below).

![Incident details](image)

**Note:** Pause conditions are not compatible with Relative Durations.

**Time display**

There are three interfaces that display record information over time: reports and performance analytics, timeline pages, schedule pages.
Report example

You can visualize data in two ways:

- **Reporting** enables users to generate charts from data within the platform in a variety of formats. Reporting is available as a standard part of the platform and offers snapshotting of current data.
- **Performance Analytics** enables you to track and aggregate data over time, such as to 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 Get licensed Performance Analytics.

Timeline pages

Timeline pages example
Timeline pages allow for easy definition of linear timelines from records with time information.

Schedule pages

Time-related functionality

There are a number of different functionalities that allow for tracking time and leveraging that information across applications.

Time Fields

Time can be stored in different ways in records. Understanding how time is stored underlies use of all of the time functions.

For more information, see: Use Date and Time Fields.
Time Zones

All times are stored in the platform in Universal Coordinated Time. They are displayed globally based on the system time zone, but are displayed to users in their local time zone according to user settings. Time zone information is important to keep track of to avoid calculation errors or confusing outputs.

All dates and times gathered through web services display in GMT. Data inserted using a web service uses the active user’s time zone or the system time zone if the active user does not have a time zone specified.

Schedules

Schedules are rules which include or exclude ranges of time for certain time-related functionality. For example, schedules can restrict SLAs to only count time during business hours.

Displaying Time

There are a number of useful user interfaces that help represent time visually.
For more information, see Displaying Time.

Viewing Logs

Logs within the system provide historical information as to what occurred in the instance when.

Scheduling Events

These functionalities allow other functionality to be triggered at particular times, or in response to specific events.
For more information, see Schedule Events.

Timing Functionality

These functions gather information with regards to duration. They answer the question "How long?", and can time events based off of that information.
For more information, see Timing Functionality.

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 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){
  var min = -1;
  var max = -1;
  var minID = "";
  var maxID = "";
  if (table == "rm_release_scrum"){
    var 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 gr = new GlideRecord("rm_release_sprint");
            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, ""];
},
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'
Use the following two functions to obtain the correct start and end dates in the three example script includes provided for reference.

```javascript
getTimeMs: function(date){
    return new ScheduleDateTime(date).getMS();
}

getTimeObject: function(timeMS) {
    var gdt = new GlideDateTime();
    gdt.setNumericValue(timeMS);
    return gdt;
}
```

**Set an inactivity monitor**

An inactivity monitor triggers an event for a task record if 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 are defined for the monitor but have not been met when you update the task record, the monitor is not restarted. 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`). The inactivity monitor does not automatically specify further actions, so either an **email notification** or script action must be defined to drive further action.

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.
6. Specify an **Order** if multiple inactivity monitors might have their conditions met for a given record - the one with the lowest order will be used.
7. Click **Save**.

**Note:** If conditions are changed on an inactivity monitor, the monitor stops tracking previously tracked records. An inactivity monitor does not track records that were 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.
System scheduler

The System Scheduler application contains two separate engines for scheduling: the Scheduled Jobs engine and the Schedules engine.

Scheduled Jobs:
Scheduled Jobs performs any work that must be done 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 front end for scheduling work. Use this module to create new scheduled jobs.

For more information, see Create a Scheduled Job.

Schedules:
Schedules are rules which include or exclude time on a calendar. They are used by service levels, inactivity monitor, and group on-call rotation. For instance, a schedule can be defined to restrict service levels to only apply to weekdays during business hours, or to 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 either a particular time, or on a recurring schedule.

These kinds of tasks can be automated:
- Run and distribute a report
- Generate a record (incident, change, configuration item, etc.) from a template
- Run a business rule and do whatever the rule contains
- Scheduling at the end of the month
- Scheduling for weekdays
- Executing scheduled jobs from scripts
Scheduled job states

A scheduled job can be in any one of the following states.

**Ready**
The job is ready to run at the next scheduled interval.

**Running**
The job is in the process of carrying out a task.

**Queued**
The job has been added to the scheduler queue and is waiting to run.

**Error**
An error occurred in running the job.

Schedule a report

Scheduled reports are distributed via email.

Roles required: admin or schedule_admin

Scheduled reports created by an individual whose user account is deactivated might not display any data. To ensure that the desired data is displayed, 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name to identify this scheduled job.</td>
</tr>
<tr>
<td>Report</td>
<td>A reference to the report to be scheduled. Calendar, Pivot Table, Map and Single Score reports are not supported for automatic emailing.</td>
</tr>
<tr>
<td>Users</td>
<td>The users to send the report to at the scheduled date and time. The user must have Notification set to <strong>Enabled</strong> on their user record to receive reports. To force users to receive emails, use the <strong>Email Addresses</strong> field.</td>
</tr>
<tr>
<td>Groups</td>
<td>The groups to send the report to at the scheduled date and time.</td>
</tr>
<tr>
<td>Email addresses</td>
<td>Any other email addresses to send the report to, separated by commas. These emails will always receive the report, even if there's a matching user record for that address that says <strong>Do not notify</strong>.</td>
</tr>
<tr>
<td>Active</td>
<td>If true, this report will be sent at the scheduled date and time.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Run</td>
<td>The type of schedule to send the report on. Choices are:</td>
</tr>
<tr>
<td></td>
<td>- Daily</td>
</tr>
<tr>
<td></td>
<td>- Weekly</td>
</tr>
<tr>
<td></td>
<td>- Monthly</td>
</tr>
<tr>
<td></td>
<td>- Periodically</td>
</tr>
<tr>
<td></td>
<td>- Once</td>
</tr>
<tr>
<td>Day</td>
<td>- If Run is Weekly, the day of the week</td>
</tr>
<tr>
<td></td>
<td>- If Run is Monthly, the day of the month.</td>
</tr>
<tr>
<td>Repeat Interval</td>
<td>If Run is Periodically, the duration between each scheduled report. The duration can be days, hours, or minutes.</td>
</tr>
<tr>
<td>Time</td>
<td>If Run is Weekly or Monthly the time of day, on a 24 hour clock.</td>
</tr>
<tr>
<td>Starting</td>
<td>The date and time of the first scheduled report.</td>
</tr>
<tr>
<td>Priority</td>
<td>The numerical priority of a scheduled job. Set essential jobs to a priority value below 100 and nonessential jobs to a priority above 100. If 70% or more of all scheduled jobs are Overdue, any jobs marked with a value above 100 do not run.</td>
</tr>
<tr>
<td>Subject</td>
<td>The subject line for the email.</td>
</tr>
<tr>
<td>Introductory Message</td>
<td>The body of the email.</td>
</tr>
<tr>
<td>Run as</td>
<td>The user creating and running the scheduled job. To have the scheduled job assigned to system behavior instead of the person creating the scheduled job, create a system or dummy user and add that user to this field.</td>
</tr>
<tr>
<td>Type</td>
<td>The file-type of 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>Include Detail</td>
<td>If checked, will include details on the records in the report.</td>
</tr>
<tr>
<td>Zip Output</td>
<td>If checked, the report will be compressed in a .zip file.</td>
</tr>
</tbody>
</table>

As a workaround for scheduling calendar and pivot table reports for email distribution, consider using the publish option. Publish creates a URL for the report and displays the address above the report form. You can create an email notification with this URL and send the link to people who need to see the report, or you can send the url for the calendar report to a distribution list.
## Schedule a script execution

Non-conditional and conditional scripts can be scheduled.

1. Navigate to **System Definition > Scheduled Jobs**.
2. Click **New**.
3. Select **Automatically run a script of your choosing**.
4. Populate the following fields:

### Schedule script execution

<table>
<thead>
<tr>
<th>Field</th>
<th>Input Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name to identify this scheduled script execution</td>
</tr>
<tr>
<td>Active</td>
<td>If true, the script will be executed at the scheduled date and time.</td>
</tr>
<tr>
<td>Run</td>
<td>The type of schedule to execute the script on. Choices are:</td>
</tr>
<tr>
<td></td>
<td>- Daily</td>
</tr>
<tr>
<td></td>
<td>- Weekly</td>
</tr>
<tr>
<td></td>
<td>- Monthly</td>
</tr>
<tr>
<td></td>
<td>- Periodically</td>
</tr>
<tr>
<td></td>
<td>- Once</td>
</tr>
<tr>
<td>Day</td>
<td>• If Run is <strong>Weekly</strong>, the day of the week</td>
</tr>
<tr>
<td></td>
<td>• If Run is <strong>Monthly</strong>, the day of the month.</td>
</tr>
<tr>
<td>Repeat Interval</td>
<td>If Run is <strong>Periodically</strong>, the duration between each script execution.</td>
</tr>
<tr>
<td>Time</td>
<td>If Run is <strong>Daily</strong>, <strong>Weekly</strong>, or <strong>Monthly</strong>, the time of day, based on a 24 hour clock.</td>
</tr>
<tr>
<td>Starting</td>
<td>The date and time of the first scheduled script execution.</td>
</tr>
<tr>
<td>Application</td>
<td>The application that contains the script.</td>
</tr>
<tr>
<td>Conditional</td>
<td>If checked, the entity will only be executed if certain conditions are met.</td>
</tr>
<tr>
<td>Condition</td>
<td>If <strong>Conditional</strong> is checked, a script determines under what conditions the scheduled script is executed. The last expression of the script should evaluate to a Boolean (true/false) value.</td>
</tr>
</tbody>
</table>

**Note:** This setting does not account for Daylight Savings Time changes. For example, if you select a period of one day, this adds 24 hours to the starting time of the job. If the start time was configured during a period with Daylight Savings Time, the job executes with a one hour offset on days when that time zone is not in Daylight Savings Time.
<table>
<thead>
<tr>
<th>Field</th>
<th>Input Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run as (Optional)</td>
<td>Select another user to run the script execution as. Configure the form to</td>
</tr>
<tr>
<td></td>
<td>add this field if it is not present.</td>
</tr>
<tr>
<td>Run this script</td>
<td>The script to run at the scheduled date and time. For example, copy script</td>
</tr>
<tr>
<td></td>
<td>logic from a business rule or call a script include.</td>
</tr>
</tbody>
</table>

**Example**

The following is an example of a conditional script. This example 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');
ga.addQuery('sys_created_on', '<', gs.daysAgo(30));
ga.query();
ga.next();
ga.getAggregate('COUNT') !== '0'
```

**Schedule the generation of an entity**

You can schedule the generation of entities, which include changes, incidents, and CIs.

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>Active</td>
<td>If true, the entity will be generated at the</td>
</tr>
<tr>
<td></td>
<td>scheduled date and time.</td>
</tr>
<tr>
<td>Run</td>
<td>The type of schedule to generate the entity on.</td>
</tr>
<tr>
<td></td>
<td>Choices are:</td>
</tr>
<tr>
<td></td>
<td>· Daily</td>
</tr>
<tr>
<td></td>
<td>· Weekly</td>
</tr>
<tr>
<td></td>
<td>· Monthly</td>
</tr>
<tr>
<td></td>
<td>· Periodically</td>
</tr>
<tr>
<td></td>
<td>· Once</td>
</tr>
<tr>
<td>Day</td>
<td>· If Run is Weekly, the day of the week</td>
</tr>
<tr>
<td></td>
<td>· If Run is Monthly, the day of the month.</td>
</tr>
<tr>
<td>Repeat Interval</td>
<td>If Run is Periodically, the duration between</td>
</tr>
<tr>
<td></td>
<td>each scheduled generation.</td>
</tr>
<tr>
<td>Time</td>
<td>If Run is Weekly or Monthly the time of day,</td>
</tr>
<tr>
<td></td>
<td>on a 24 hour clock.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting</td>
<td>The date and time of the first scheduled generation.</td>
</tr>
<tr>
<td>Conditional</td>
<td>If checked, the entity will only be generated if certain conditions are met.</td>
</tr>
<tr>
<td>Condition</td>
<td>If Conditional is checked, a script determines under what conditions the scheduled script is executed. The last expression of the script should evaluate to a Boolean (true/false) value.</td>
</tr>
<tr>
<td>Generate this</td>
<td>A reference to a template for a record.</td>
</tr>
</tbody>
</table>

### 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 will not be executed in months (like February) which are shorter than those dates.
- If an event is scheduled for the 31st, it will be executed 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 will run on February 28th or February 29th in a leap year.

#### Weekday schedules

For scheduled scripts, use the following script to run only on weekdays:

```javascript
(function isWeekday() {
  var 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
```
This script can be run 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, the system does not automatically create Schedule Item (sys_trigger) records 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.

#### Create a scheduled job

Create a scheduled job on the Schedule Job (sysauto) table (System Definition > Scheduled Jobs).

Create all new scheduled jobs using this method. Some existing scheduled jobs are found on the Schedule Item (sys_trigger) table (System Scheduler > Scheduled Jobs). Do **not** create new scheduled jobs on the Schedule Item table.

1. Navigate to **System Definition > Scheduled Jobs**.
2. Click **New**.
3. Select the appropriate type of scheduled job.

The fields presented will depend on the type of scheduled job required.

#### View a schedule item

Schedule items are individual instances of a scheduled job. You can view them from the system scheduler.

1. Navigate to **System Scheduler > Today’s Scheduled Jobs**. The table displays each schedule item that will be run.
Note: It is usually inadvisable to modify the schedule items themselves. It is best to modify the scheduled jobs that contain them.

Event scheduling

There are a variety of tools available 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 allows changes to be proposed and viewed through a timeline.

On-call rotation

The Group On-Call Rotation Plugin allows a schedule to be defined to determine what users are primary contacts during particular hours of the day.

Scheduled reports

Once reports are defined, they can be scheduled to be emailed 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 can be 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 which can be set to be automatically performed at a specific date and time, or on a repeating basis.

Event registry

Events can be used 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, used to trigger the script action Knowledge View to 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 incident commented email notifications.

Inactivity Monitors:

An inactivity monitor triggers an event if a record has not been updated for a defined length of time.

Script Actions:

Script actions are scripts which are triggered when an event is recorded in the log. In that way, scripts can be set to be performed whenever a particular activity occurs in the platform, rather than at a particular time (like scheduled jobs) or in response to particular conditions (like **Business rules**).

Notifications:
Events are also used 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. Complete the Event Registration form as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Input Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of your new event.</td>
</tr>
<tr>
<td>Table</td>
<td>The 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 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: The list shows only tables and database views that are in the same scope as the event.

Timeline pages

Use timeline pages to track any activity bounded by two dates, such as the start and end date of a change request or the open and close date of an incident. 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.
Timeline View

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

ITIL users can view timelines associated with any task record where the metrics are set to display as timeline records (by default, only Incident records display timeline metrics). ITIL users can select the Metrics Timeline context menu UI action to view the Assigned to duration and the State duration metric timelines.

1. Navigate to active task record, such as an incident.
2. Right-click the banner, and select Metrics Timeline.

To allow non-administrators to view other timelines, create a custom module.

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>Enter a unique name that describes the function of this timeline. For example, High Priority Change Requests.</td>
</tr>
<tr>
<td>Table</td>
<td>Select the name of the table associated with this timeline, such as Change Request [change_request].</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. The timeline begins with the span for the record with the earliest start date from this field, after the filter and sort order are applied. For example, you can select Updated as the start date field and start 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>Select a 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 the filter and sort order are applied. 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.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show left pane</td>
<td>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.</td>
</tr>
<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 Span text fields 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 Number and Short description. 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 Category, Assigned to, and Due date.</td>
</tr>
<tr>
<td>Filtering and Sorting</td>
<td>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.</td>
</tr>
<tr>
<td>Perform custom sort?</td>
<td>Select this check box to enable custom sorting. Configure the sort order by selecting fields in the Sort by and Sort by order fields.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</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>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>Range calculator</td>
<td>Specify a script include that <strong>calculates</strong> 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 the timeline page span styles

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition</td>
<td>Create a Condition Builder to filter the results that appear in the timeline.</td>
</tr>
<tr>
<td>Label color</td>
<td>Select the color for the text under each span.</td>
</tr>
<tr>
<td>Label decoration</td>
<td>Select a character style for the text under each span: Bold, Italic, Underline, or Line-through.</td>
</tr>
<tr>
<td>Order</td>
<td>Enter a 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>Select the color of each span.</td>
</tr>
<tr>
<td>Timeline page</td>
<td>Select the 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.

This can be used to 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, a sub item might be sprints, and a sprint might have stories as a sub item.

To create a new 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 High Priority Changes.</td>
</tr>
<tr>
<td>Field</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Table</td>
<td>Select the table called by this timeline. The selected table must have at least one reference field to the table 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>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. If multiple reference fields are available, choose the reference field that forms part of the hierarchy to be modeled by this timeline. 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 for the sub item. ServiceNow uses the parent reference column to determine which records are displayed at each level of the timeline.</td>
</tr>
<tr>
<td>Display Options</td>
<td></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 will update the color to light blue.</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 Number and Short description. The span labels also appear in the left pane if the timeline displays the left pane.</td>
</tr>
<tr>
<td>Tooltip text fields</td>
<td>Select fields from the specified table to have those values appear as tooltips. For example, you might select Category, Assigned to, and Due date.</td>
</tr>
<tr>
<td>Filtering and Sorting</td>
<td></td>
</tr>
<tr>
<td>Condition builder</td>
<td>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.</td>
</tr>
<tr>
<td>Field</td>
<td>Definition</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<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 Tooltip text fields 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>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>Restriction</td>
<td>Specify the behavior when dragging a child span (available only if no <strong>Range calculator</strong> was specified for the parent timeline page).</td>
</tr>
<tr>
<td></td>
<td>- <strong>None</strong>: No restriction is in place.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Restrict by parent</strong>: Child span can be moved only within the time frame defined by the parent span.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Update parent</strong>: Parent span is updated when the child span is moved outside the time frame defined by the parent span.</td>
</tr>
</tbody>
</table>

**Display a metric as a timeline**

Administrators can allow 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

Make selected timelines available to users by creating a custom module within an application and defining the roles that can access it.

To permit these users to update task records directly from the timeline, configure the timeline to allow span dragging.

Note: Timelines delivered by a custom module are not entirely dynamic. The left pane, the summary pane, the auto-refresh feature, and the grid lines are not dynamic and do not reflect changes made to the timeline record after the module link is created. However, the data represented by the spans, the 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><strong>Field</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Enter the name of the module as it will appear in the navigation pane. For example, you might use Planning Timeline.</td>
</tr>
<tr>
<td>Order</td>
<td>Enter a number to determine the sequence in which this condition will be evaluated if more than one matching condition exists. Conditions with a lower order are evaluated first.</td>
</tr>
<tr>
<td>Application</td>
<td>Select the application for the new module.</td>
</tr>
<tr>
<td>Hint</td>
<td>Enter a 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>Select this check box to enable the module for the roles defined. Clear this check box to disable the module for all users.</td>
</tr>
<tr>
<td>Image</td>
<td>Select an appropriate icon to appear with the module name.</td>
</tr>
<tr>
<td>Link type</td>
<td>Select Timeline Page. When this link is selected, the Timeline Page field appears.</td>
</tr>
<tr>
<td>Timeline Page</td>
<td>Select the 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>Select the roles that can access this module.</td>
</tr>
<tr>
<td>Override application menu roles</td>
<td>Select this checkbox to show this module 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.

**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
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.

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.

**Focusing and Zooming on a Span**

<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.
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.

![Time worked: 03:13:18 / 00:00:10](image)

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 [task_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.

Time zones

All times are stored in Coordinated Universal Time (UTC). They are displayed globally based on the system time zone, but are displayed to users in their local time zone according to user preferences.
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 machine. Depending on how the machine 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 a time zone is specified based on location (for example, America/Los_Angeles), the system automatically adjusts for daylight saving time. If a time zone is specified based on the name of a time zone (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 TimeZone class

The Now Platform supports all time zones in the Java TimeZone class. To view a listing of these time zones:

1. In the Type filter text field, type sys_user.list.
2. Open one of the user records in the listing.
3. Right-click the Timezone field and select Show Choices.
   The resulting list is a complete listing of available Timezone IDs.

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:

![Use the following time zone for SLA:]

- The caller's time zone
- The SLA definition's time zone
- The CI's location's time zone
- The task's location's time zone
- The caller's location's time zone

Time zone for service level agreements

Some special considerations:

- If **The caller's time zone** is selected, unpredictable behavior can occur if the caller does not have a time zone defined.
- If **The SLA definition's time zone** is selected, the time zone must be manually defined on the SLAs form.

Time zone in scripting

When scripting on the server, there are several GlideSystem date and time functions used to obtain time values. For more information about specific methods and to learn the format in which each returns the requested time, see the .

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). Upon the next login, the time zone setting reverts to the system default, or user profile setting for time zone.

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.

---

**Note:** The time zone choice MUST be equal to a valid Java/IANA time zone name. If it is not, then the time zone choice is effectively UTC/GMT.

### 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.

Set a system time zone

Set your system time zone with a system property.

All times are stored in Coordinated Universal Time (UTC), but are displayed globally based on system time zone (glide.sys.default.tz) or, if specified, according to user preference.

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 input field is blank. If no time zone is defined 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 user is assigned the selected time zone and does not use the system time zone anymore.

Search administration

The system uses the Zing search engine to manage search functionality.

Explore
- Now Platform release notes
- Upgrade to London
- Features of search administration
- Features of Zing text indexing and search engine

Set up
- Set global text search properties
- Zing can include attachments in search results
- Zing can expand search results with synonyms

Administer
- Zing indexes words
- Global text search finds records from multiple tables
- List search finds records from the current table

Use
- Boolean operators allow conditional search results
- Quotation marks allow exact phrase searches

Develop
- Developer training
- Developer documentation

Troubleshoot and get help
- Ask or answer questions in the Platform forum
- Search the HI Knowledge Base for known error articles

© 2019 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.
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><strong>Zing text indexing and search engine</strong></td>
<td>Index and search record data by table.</td>
<td>• Enable text indexing for a table</td>
<td>Active</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Zing can expand search results with synonyms</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Zing can include attachments in search results</td>
<td></td>
</tr>
<tr>
<td><strong>Contextual search displays matching knowledge results</strong></td>
<td>Display search results on forms and record producers when users enter text in a field.</td>
<td>• Define search fields on a form</td>
<td>Active</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Define search context</td>
<td></td>
</tr>
</tbody>
</table>

Zing text indexing and search engine

Index and search record data by table.

Zing text search is:

- an index split into multiple database shards for parallel querying
- created entirely with ServiceNow code
- implemented purely within the relational model
- yields fast results with search engine logic
- provides search results with an emphasis on relevancy scoring
  - frequency points
  - proximity points
  - field-level scoring (such as title, metadata, and short description)

- provides search suggestions
  - Type-ahead search suggestions
  - **Did you mean**: global search suggestions

Administrators and users with the ts_admin role can configure:

- match relevance
- field weights for each table
- global stop words
- stop words for each index
- synonym dictionaries for each table
- tables with attachment indexing
By default, the system uses the Zing text indexing and search engine to search record data.

## 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 |
| **Global text search finds records from multiple tables** | Search multiple record types from a single search field. | · Add a search group  
· Enable text indexing for a table | Active |
| **Global text search displays results dynamically** | Display global text search results for each table as Zing generates them. | · Add a search group  
· Revert to the legacy global search UI | Active |
| **List search finds records from the current table** | Search records from a table list view. | · Enable text indexing for a table  
· Regenerate a text index for a table | Active |
| **Zing can include attachments in search results** | Expand search results to include attachments from indexed tables. | · Index attachments on a table  
· Enable text indexing for a table | Active |
| **Zing removes stop words from queries** | Remove common words from search queries that do not produce meaningful results. | · Configure a global stop word  
· Configure a table-specific stop word | Active |
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Top tasks</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zing matches derived words with stemming</td>
<td>Convert any multiple-character search keyword to its stem form to find derived versions of the word.</td>
<td>Set localization properties, Activate a language</td>
<td>Active</td>
</tr>
<tr>
<td>Zing can expand search results with synonyms</td>
<td>Expand search results to include additional search terms.</td>
<td>Enable search synonyms, Create synonym dictionaries</td>
<td>Inactive</td>
</tr>
</tbody>
</table>

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>
<tr>
<td>UI pages</td>
<td>Create a custom UI page to search for records in a table.</td>
</tr>
</tbody>
</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 from 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.
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 text box to enter new search terms.</td>
</tr>
<tr>
<td>2. Total results</td>
<td>The total number of matching records.</td>
</tr>
<tr>
<td>3. Search group name</td>
<td>The name of the search group.</td>
</tr>
<tr>
<td>UI element</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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 ten matching records per table. The system displays a separate list for each table in the search group sorted from highest to lowest document score. By default, the system uses the table text_search list view if available. Otherwise, it displays fields with the default list view. Administrators can set the preview results limit and the search results view from the <a href="#">global text search properties</a>.</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.</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 <a href="#">Add a search group</a> 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>9. Global search box</td>
<td>The standard global search text box.</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.

Sample search result listing

1. **Update /etc/network/interfaces to include name servers 8.8.8.8 & 8.8.4.4**
2. **Number: CHG0000072 | Type: Normal | State: Authorize | Planned start date: 2017-06-19 19:30:00 | Priority: High**
   **Requested by: System Administrator | Assigned to: Bow Ruggeri**
3. **We need to add additional redundant name servers to Linux100, Linux101 and PS LinuxApp01**
### 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 ‘No title’ 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>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</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>
<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 Contacts 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>Enable Global Text Search</td>
<td>Default value is true. Clear this option to disable the global text search capability.</td>
</tr>
<tr>
<td>glide.ui.text_search.enable</td>
<td></td>
</tr>
<tr>
<td>List of roles (comma-separated) that can use the Global Text Search capability.</td>
<td>Default value is itil, text_search_admin, admin. Add a role to enable it to use search.</td>
</tr>
<tr>
<td>glide.ui.can_search</td>
<td></td>
</tr>
<tr>
<td>List of tables (comma-separated) that will not appear as options when setting up Global Text Search tables.</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>glide.ui.no_text_search</td>
<td></td>
</tr>
<tr>
<td>Number of Global Text Search matches returned per table.</td>
<td>Default value is 10. Users can click through to see all results for a specific table.</td>
</tr>
<tr>
<td>glide.ui.text_search.rowcount</td>
<td></td>
</tr>
<tr>
<td>Global Text Search background color for Knowledge Base results.</td>
<td>This property only applies to the legacy global search results page. Default value is #FFFFDD.</td>
</tr>
<tr>
<td>css.textsearch.kb.background.color</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>css.textsearch.catalog.background.color</td>
<td>This property only applies to the legacy global search results page. Default value is #F0F7F9.</td>
</tr>
<tr>
<td>glide.ui.text_search.match_view</td>
<td>Default value is blank.</td>
</tr>
<tr>
<td>glide.ui.text_search.view</td>
<td>Default value is the text_search view. If you do not have a text_search view, you can create it.</td>
</tr>
<tr>
<td>glide.ir.query_method</td>
<td>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 Property 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>glide.ts.stemming_language</td>
</tr>
<tr>
<td>Default value is <strong>English</strong></td>
<td>- The system supports stemming in English, German, and French.</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 though 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**.

Disable the junk filter

By default, Zing does not index or search for 2-digit numbers and single character words (unless they are Chinese or Japanese characters). You can turn off this filter for a table.

For example, to have the ability to search for error 92 in the knowledge base, turn off junk filtering for `kb_knowledge`.

1. Navigate to **System Definition > Dictionary**.
2. Open the dictionary entry for the table.
3. In the **Attributes** field, enter `text_index_filter_junk=false`.
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.
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.
6. Navigate to **System Definition > Text Indexes**.
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.
   The entire list of properties in the System Properties (sys_properties) table appears.
2. Click **New**.
3. 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.

![Image of search tips and preferences]

**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"
<table>
<thead>
<tr>
<th>User preference</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Label</strong></td>
<td><strong>Use remembered expand / collapse preferences</strong></td>
</tr>
<tr>
<td><strong>Preference</strong></td>
<td><strong>ts.remember.expanded</strong></td>
</tr>
<tr>
<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>
<td></td>
</tr>
<tr>
<td><strong>Label</strong></td>
<td><strong>Show list of tables with no search matches</strong></td>
</tr>
<tr>
<td><strong>Preference</strong></td>
<td><strong>ts.show_negative_result_info</strong></td>
</tr>
<tr>
<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>
<td></td>
</tr>
<tr>
<td><strong>Label</strong></td>
<td><strong>Show selectable search groups</strong></td>
</tr>
<tr>
<td><strong>Preference</strong></td>
<td><strong>ts.show_search_groups</strong></td>
</tr>
<tr>
<td>Shows or hides the search group check box row.</td>
<td></td>
</tr>
<tr>
<td><strong>Label</strong></td>
<td><strong>Show groups with no search matches</strong></td>
</tr>
<tr>
<td><strong>Preference</strong></td>
<td><strong>ts.show_empty_groups</strong></td>
</tr>
<tr>
<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>
<td></td>
</tr>
<tr>
<td><strong>Label</strong></td>
<td><strong>Return task record if searching for exact number</strong></td>
</tr>
<tr>
<td><strong>Preference</strong></td>
<td><strong>ts.match</strong></td>
</tr>
<tr>
<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>
<td></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.

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.

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.
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.

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.
### INCIDENT CONDITIONS

All of these conditions must be met

Keywords are

or

New Criteria

### RELATED LIST CONDITIONS

<table>
<thead>
<tr>
<th>Incident ID</th>
<th>Date/Time</th>
<th>Description</th>
<th>Caller</th>
</tr>
</thead>
<tbody>
<tr>
<td>INC0000051</td>
<td>2016-11-15 12:48:32</td>
<td>Manager can't access SAP Controlling application</td>
<td>Joe Emp</td>
</tr>
<tr>
<td>INC0000052</td>
<td>2016-11-15 12:48:40</td>
<td>SAP Financial Accounting application appears to be down</td>
<td>Bud Rich</td>
</tr>
<tr>
<td>INC0000055</td>
<td>2016-11-15 20:47:23</td>
<td>SAP Sales app is not accessible</td>
<td>Carol Cole</td>
</tr>
<tr>
<td>INC0000053</td>
<td>2016-11-15 12:48:46</td>
<td>The SAP HR application is not accessible</td>
<td>Margaret</td>
</tr>
<tr>
<td></td>
<td>2015-11-02</td>
<td>SAP Materials</td>
<td></td>
</tr>
</tbody>
</table>
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 from global text searches.

All global text search interfaces support boolean operators.

- Global text search field
- Knowledge Base search
- List search for text

For Knowledge Base searches, if the 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` property.

**Note:** Boolean operators are case-sensitive. For example, OR is an operator while or is a search term that may be a stop word.

Also, if you type a string that happens to contain a Boolean operator, rather enter it into the search interface, it is evaluated as part of the text string, rather than as an operator. For example, if you actually type "email password" OR email, it is interpreted as the full text string "email password" OR email. In this case, it searches for that actual text string, but does not consider OR to be a Boolean operator, yielding significantly different results in Knowledge Base searches.
### 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 <strong>email password</strong> or just <strong>email</strong>, search for <strong>email password</strong> OR email OR <strong>email password</strong></td>
</tr>
<tr>
<td>Operator</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>AND</td>
<td>Finds a match if all terms exist in a document (an intersection of sets). For example, to find documents that contain &quot;CPU load&quot; and &quot;10 minutes&quot;, search for &quot;CPU load&quot; AND &quot;10 minutes&quot;. 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 &quot;email server down&quot; to (Keywords (are) (email) AND (Keywords (are) (server) AND (Keywords (are) (down)).</td>
</tr>
<tr>
<td>NOT, minus (-), or exclamation point (!)</td>
<td>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 &quot;CPU load&quot; NOT &quot;10 minutes&quot;, &quot;CPU load&quot; -&quot;10 minutes&quot;, or &quot;CPU load&quot; &quot;$10 minutes&quot;. The NOT operator cannot be used with just one term. For example, the following search returns no results: NOT &quot;10 minutes&quot;. 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.</td>
</tr>
</tbody>
</table>

**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.

• Lists (text searches of all fields)
• Reference fields

**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.

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. 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.

**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.
Divide documents among index shards

**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, \( \text{(contains)(wifi)(AND)(contains)(network)} \).

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
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.

<table>
<thead>
<tr>
<th>Doc</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>60</td>
<td>10</td>
</tr>
<tr>
<td>50</td>
<td>8</td>
</tr>
<tr>
<td>100</td>
<td>3</td>
</tr>
<tr>
<td>10</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Doc</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>81</td>
<td>11</td>
</tr>
<tr>
<td>91</td>
<td>6</td>
</tr>
<tr>
<td>101</td>
<td>5</td>
</tr>
<tr>
<td>11</td>
<td>4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Doc</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>99</td>
<td>12</td>
</tr>
<tr>
<td>19</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Doc</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>60</td>
<td>10</td>
</tr>
<tr>
<td>50</td>
<td>8</td>
</tr>
<tr>
<td>91</td>
<td>6</td>
</tr>
<tr>
<td>19</td>
<td>6</td>
</tr>
<tr>
<td>101</td>
<td>5</td>
</tr>
<tr>
<td>11</td>
<td>4</td>
</tr>
<tr>
<td>100</td>
<td>3</td>
</tr>
<tr>
<td>10</td>
<td>1</td>
</tr>
</tbody>
</table>
**Zing filters search results with access controls**

Filter 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.
### System Properties - 14

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
<th>Type</th>
<th>Description</th>
<th>Updated</th>
<th>Updated by</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.smtp.default_retry</td>
<td>true</td>
<td>true</td>
<td>Resend email when unknown SMTP error code...</td>
<td>2012-01-27</td>
<td>admin</td>
</tr>
<tr>
<td>glide.smtp.fail_message_ids</td>
<td>500,501,502,903,504,550,551,552,553,554</td>
<td>string</td>
<td>Do not resend email if these SMTP error codes...</td>
<td>2012-01-27</td>
<td>admin</td>
</tr>
<tr>
<td>glide.smtp.defor_retry_ids</td>
<td>421,460,461,462</td>
<td>string</td>
<td>Resend email if these SMTP error codes...</td>
<td>2012-01-27</td>
<td>admin</td>
</tr>
<tr>
<td>glide.smtp.server</td>
<td>relay</td>
<td>string</td>
<td>Outgoing (SMTP) mail server. Also used as...</td>
<td>2013-04-01</td>
<td>admin</td>
</tr>
<tr>
<td>glide.smtp.default_suffix</td>
<td>relay</td>
<td>string</td>
<td>Default gateway address for any outbound...</td>
<td>2007-03-28</td>
<td>glide.maint</td>
</tr>
<tr>
<td>glide.smtp.user</td>
<td>string</td>
<td>string</td>
<td>Incoming (POP) mail account name, if different...</td>
<td>2013-01-04</td>
<td>guest</td>
</tr>
<tr>
<td>glide.smtp.user</td>
<td>string</td>
<td>string</td>
<td>User email (eg. <a href="mailto:helpdesk@company.com">helpdesk@company.com</a>) the...</td>
<td>2013-01-04</td>
<td>guest</td>
</tr>
<tr>
<td>glide.smtp.auth</td>
<td>false</td>
<td>true</td>
<td>Authenticate with the SMTP server using...</td>
<td>2010-06-23</td>
<td>dico</td>
</tr>
<tr>
<td>glide.smtp.active</td>
<td>true</td>
<td>true</td>
<td>Enable email sending (SMTP)...</td>
<td>2009-06-25</td>
<td>glide.maint</td>
</tr>
<tr>
<td>glide.smtp.fail_message_ids</td>
<td>500,501,502,903,504,550,551,552,553,554</td>
<td>string</td>
<td>Do not resend email if these SMTP error codes...</td>
<td>2012-01-27</td>
<td>admin</td>
</tr>
<tr>
<td>glide.smtp.defor_retry_ids</td>
<td>421,460,461,462</td>
<td>string</td>
<td>Resend email if these SMTP error codes...</td>
<td>2012-01-27</td>
<td>admin</td>
</tr>
<tr>
<td>glide.smtp.server</td>
<td>relay</td>
<td>string</td>
<td>Outgoing (SMTP) mail server. Also used as...</td>
<td>2013-04-01</td>
<td>admin</td>
</tr>
<tr>
<td>glide.smtp.default_suffix</td>
<td>relay</td>
<td>string</td>
<td>Default gateway address for any outbound...</td>
<td>2007-03-28</td>
<td>glide.maint</td>
</tr>
<tr>
<td>glide.smtp.user</td>
<td>string</td>
<td>string</td>
<td>Incoming (POP) mail account name, if different...</td>
<td>2013-01-04</td>
<td>guest</td>
</tr>
<tr>
<td>glide.smtp.user</td>
<td>string</td>
<td>string</td>
<td>User email (eg. <a href="mailto:helpdesk@company.com">helpdesk@company.com</a>) the...</td>
<td>2013-01-04</td>
<td>guest</td>
</tr>
</tbody>
</table>
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 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.

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.

Following the example above, each time the string "database server" appears in a document, it is awarded 100 (10^2) sequence points. Likewise, each time the string "distributed database server" appears in a document, it is awarded 1000 (10^3) sequence points.

Zing awards sequence points as 10^x, where x is the number of search terms that appear in sequence. If the sequence appears in a field that is weighted, Zing applies a multiplier to the sequence points based on the value of the ts_weight attribute for the field. The sequence points use the calculation (10^x * weight of the field).

Weight points

Zing awards a document more points if the field in which it appears is weighted. Zing applies a multiplier to frequency points based on the value of the ts_weight attribute for the field.

By default, each field has a weight of 1. A field with a weight of 50 (ts_weight=50) would add 50 points each time a search term appeared in the field. The maximum possible weight value is 255.

By default, the system elevates the scoring weight of knowledge record numbers, knowledge short descriptions, task record numbers, and task short descriptions.

- kb_knowledge.number = 50
- kb_knowledge.short_description = 10
- kb_knowledge.meta = 10
- task.number = 50
- task.short_description = 10

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.

Note: This task requires that you regenerate an index and therefore should be done with system performance in mind. Regenerating an index may take a while to complete depending on table size and other factors. You may notice performance degradation or incomplete search results while the system regenerates the index.

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 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 <em>Zing indexes punctuation as part of some words</em>.</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>Punctuation</td>
<td>Indexed to find</td>
<td>Search behavior</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------</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 <code>PROD-10-987</code> locates exact matches to the search term.</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 <code>u.s.a.</code> locates matches to usa or u.s.a. Note that wildcard searches may affect acronym handling. In another example, a search for <code>u.s.*</code> may yield better results than a search for <code>u.s*</code>.</td>
</tr>
<tr>
<td>Host names</td>
<td></td>
<td>Zing locates sequences of letters and numbers separated only by periods. For example, a search for <code>en.myhost123.com</code> locates exact matches to the search term.</td>
</tr>
<tr>
<td>IP addresses</td>
<td></td>
<td>Zing locates numbers that follow a typical IPv4 address pattern. For example, a search for <code>10.0.0.1</code> locates exact matches to the search term.</td>
</tr>
<tr>
<td>Product numbers</td>
<td></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 <code>PROD.10.987</code> locates exact matches to the search term.</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 <code>Google+</code> locates exact matches to the search term.</td>
</tr>
</tbody>
</table>
**Punctuation** | **Indexed to find** | **Search behavior**
--- | --- | ---
Underscores (_-) | Product numbers | 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.

**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 <code>title</code> attribute of any HTML element. This is separate from the <code>title</code> 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 <code>href</code> 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**.

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**.

<table>
<thead>
<tr>
<th>Table Name</th>
<th>Column Name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>sys_user</td>
<td>accumulated_roles</td>
<td>string</td>
</tr>
<tr>
<td>sys_user</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>sys_user</td>
<td>building</td>
<td>cmn_b</td>
</tr>
<tr>
<td>sys_user</td>
<td>calendar_integration</td>
<td>integer</td>
</tr>
</tbody>
</table>

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.

**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.
<table>
<thead>
<tr>
<th>Table</th>
<th>Task [task]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>Ready</td>
</tr>
<tr>
<td>Indexed rows</td>
<td>463</td>
</tr>
<tr>
<td>Unique terms</td>
<td></td>
</tr>
<tr>
<td>Total terms</td>
<td></td>
</tr>
<tr>
<td>Disable synonym</td>
<td></td>
</tr>
<tr>
<td>Partial Match Rule</td>
<td></td>
</tr>
</tbody>
</table>

Generate Text Index

The text index will be generated in the background so that you can continue other work while it is being created. If this table does not have a text index, one will be created after the dictionary text index flag is set to true. Upon completion, the system will send you a confirmation email unless you specify otherwise below.

Upon completion:
- [ ] Email me: admin@example.com
- [ ] Do not notify me

Text Index Specifics

Table name: task

Cancel | 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:

   ```java
   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:

   ```java
   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:

   ```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 an index if you no longer want the search engine to return results for table.

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 an index if you no longer want the search engine to return results for a specific field.

1. Navigate to a form containing the field.
2. Right-click the field label and select Configure Dictionary.
3. Add no_text_index=true to the Attributes field. Separate multiple attributes with a comma (with no spaces).
4. Click Update.
   The system no longer indexes or queries the field 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>
<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.

---

**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.

<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 <strong>ja</strong> 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.
Sample search including 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.

Zing supports indexing and searching these attachment file types.

- .doc
- .htm
- .html
- .ini
- .pdf
- .ppt
- .reg
- .txt
- .xls
- .docx
- .dotx
- .dot
- .pptx
- .potx
- .pot
- .xlsx
- .xltx
- .xlt

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. Click the Attributes tab.
4. Click New and add the following values.

<table>
<thead>
<tr>
<th>Attribute values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
</tr>
<tr>
<td>Attribute</td>
</tr>
<tr>
<td>Value</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.

5. Click Submit.
   The indexing process begins. When it is complete, attachments can be searched on that table.
6. Optional: To disable attachment indexing, remove the attribute and click Update.

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 stop 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 ServiceNow 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**, 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.

### Synonym dictionary form

<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.

### Synonym set form

<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.
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.

**Note:** You can only view the debug output on a table view (_list.do). You cannot view it on a UI page itself.

### Installed with Zing

Several types of components are installed with Zing.

#### Tables 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>
<tr>
<td>ts_attachment</td>
<td>System tables that support Zing. Extending or modifying these tables is not recommended.</td>
</tr>
<tr>
<td>ts_chain_summary</td>
<td></td>
</tr>
<tr>
<td>ts_chain</td>
<td></td>
</tr>
<tr>
<td>ts_deleted_doc</td>
<td></td>
</tr>
<tr>
<td>ts_document</td>
<td></td>
</tr>
<tr>
<td>ts_index_stats</td>
<td></td>
</tr>
<tr>
<td>ts_phrase</td>
<td></td>
</tr>
<tr>
<td>ts_search_stats</td>
<td></td>
</tr>
<tr>
<td>ts_search_summary</td>
<td></td>
</tr>
<tr>
<td>ts_word_roots</td>
<td></td>
</tr>
<tr>
<td>ts_word</td>
<td></td>
</tr>
</tbody>
</table>

© 2019 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.
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 “neither index nor query”.</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>

Contextual search displays matching knowledge results

Display search results on forms and record producers when users enter text in a field.
Contextual search helps users deflect or quickly resolve their issues without involving the service desk operators. Contextual search can include results from Knowledge and other sources such as a service catalog, allowing a user to directly order a catalog item from a search.

Contextual searches are enabled for incidents by default, providing incident deflection using knowledge and social Q&A questions. This default implementation includes contextual search results for forms, record producers, and email notifications.

To define a contextual search, first define a search context to set parameters, then define where the contextual search results are to appear: in forms and in record producers.

You must have the admin role to define contextual searches and to administer contextual search functions and properties.

**Define contextual search**

You can add and configure contextual search functions for fields in forms and record producers.

For example, you can add a new contextual search capability to the Service Desk Call form, linking search to the short description in that form. This automatically provides relevant knowledge to service desk staff when they respond to calls, helping to resolve these calls more quickly.

By default, the system provides contextual search for incident record producers and the Incident form to help with *incident deflection and resolution*.

**Contextual search process flow**

Understand the steps you follow to define the contextual search process.

1. Define a search context to be available in multiple locations, setting overall values and conditions for the search results displayed.
   For example, define a search context for service desk calls that only displays search results from the Technical Solutions knowledge base.

2. Define where the contextual search results are to appear.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Forms</strong></td>
<td>You can define knowledge to be associated whenever a problem record is created. For forms, you can also provide search results with email notifications sent when a record is created. For example, automatic notifications sent when an incident is created can include knowledge search results which may help the user who raised the incident resolve the issue independently.</td>
</tr>
<tr>
<td><strong>Record producers</strong></td>
<td>Define a Create New Incident record producer to trigger a search based on text entered in the Comments field. Display the search results at the bottom of the record producer.</td>
</tr>
</tbody>
</table>

**Define search context**

Create a search context to define a contextual search, with links to define which forms and record producers use that search.

For example, define a search context for service desk calls that only displays search results from your organization's Technical Solutions knowledge base.

1. Navigate to **Contextual Search > Search Contexts**.
2. Click **New**.
3. Fill in the fields, as appropriate.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the context.</td>
</tr>
<tr>
<td>Short description</td>
<td>Summary of the context.</td>
</tr>
<tr>
<td>Searcher</td>
<td>The searcher for this context, which 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 SocialQA/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, SocialQA: Provides search results from Knowledge, Pinned Knowledge, Catalog items and Social Q&amp;A.</td>
</tr>
<tr>
<td></td>
<td>- Knowledge, Social Q&amp;A and pinned: Provides search results from knowledge articles, pinned knowledge articles and Social Q&amp;A.</td>
</tr>
<tr>
<td></td>
<td>- Pinned Knowledge only: Provides search results from pinned knowledge articles.</td>
</tr>
</tbody>
</table>

| Active     | Check box for activating the search context.                               |

4. Right-click the form header and click **Save**.
5. Optional: Click **Set As Default** to make this the default context, used if a search query does not specify a context. For example, if a search query is invoked from a script without providing a context.
6. Use the related lists to further define the search context.
   - Record Producer Configurations: define which record producers use this context.
   - Table Configurations: define which forms use this context.
   - Resource Configuration: define configurations to apply to the search context, such as restrictions on the results displayed.

**Define contextual search for a table**

Define contextual search to display search results in a table, such as the form for the Incident table.

Role required: admin
In **Contextual Search > Table Configuration**, you can configure the form that is associated with a table to display contextual search results. You specify where the search results appear, the information the results contain, and what the user can do with the results.

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 resolve the issue independently.

In the table configuration record, specify which fields on the form trigger a search. For example, contextual search in the Incident form can display search results based on text entered in the **Short description** field.

You can turn on metadata for knowledge article results to know which knowledge base the article belongs to. To turn the metadata, navigate to **Contextual Search > Properties** and select **Yes** for **Shows meta data on form contextual search results**. There are additional knowledge article metadata settings in **Knowledge > Properties** under **Knowledge Search Properties**, including whether to show the knowledge article number in the results.

1. In the **Search Context** form, open the **Table Configurations** related list and click **New**. Alternatively, navigate to **Contextual Search > Table Configuration** and click **New**.

2. Complete the form.
### Table Configuration fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>Name of the table name associated with the form, for example, Incident (incident). Note: The list shows only tables and database views that are in the same scope as the contextual search.</td>
</tr>
<tr>
<td>UI type</td>
<td>Table Configuration used in a Platform form or in Workspace.</td>
</tr>
<tr>
<td>Search context</td>
<td>Name of the search context this table configuration applies to.</td>
</tr>
<tr>
<td>Results header text</td>
<td>Label for the search results area that appears in the form.</td>
</tr>
<tr>
<td>Enable related search box</td>
<td>Check box to show the related search box (platform only) within the Contextual Search Results. When checked this option allows the user to change the search text without editing the short description (or whichever field is set as the search field).</td>
</tr>
<tr>
<td>Active</td>
<td>Check box to activate this 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 allow the user to collapse the search results in the form.</td>
</tr>
<tr>
<td>Enable preview buttons</td>
<td>Check box 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>
<tr>
<td>When to display</td>
<td>Conditions under which this search is enabled. For example, set (Active) (is) (true) to only enable the search on active knowledge articles.</td>
</tr>
<tr>
<td>Enable search as</td>
<td>Defines results to show for a different user. For more information, see Search as different users.</td>
</tr>
</tbody>
</table>

3. Open the form context menu and select **Save**. The Search Fields, Filter Configurations, and Email Configurations related lists appear. By default, a search field record is added to search on the **Short description** field.

4. Optional: To use a different search field, open the Short description record, select the field, and click **Update**.

5. Optional: Refer to the following topics to add a filter configuration.

Filter configurations are defined to map fields from two different tables to provide a more targeted search result set. You can do any of the following options:

- Create a filter configuration using mapping
- Create a filter configuration using scripting
6. Optional: Complete the following steps to define email configurations to include knowledge search results.
   a) Click **New** in the **Email Configurations** related list.
   b) Select the email notification to attach search results.
      You can select only from the notifications that are on the same table as the table configuration record.
   c) Select the field used to restrict the search results.
      For example, if you select **Opened by**, the search results include only the articles that the opened-by user can access based on user criteria.
   d) Update the **Limit** field as desired.
   e) Click **Submit**.

7. Optional: Modify the search actions that you can perform on the search result.

   The Search Action Configurations related list contains all the available Search actions available for the selected Search context. Search actions can be modified but not deleted and new actions cannot be created.

   The Search actions that can be modified are as follows:
   - **Action label**: Display label that is shown on the **Action** button in result list.
   - **Action value**: Value that is logged in to the query feedback table when the action is taken.
   - **Attachment type** (Attach actions only): Ways to attach a Knowledge article such as to embed a link to the article (recommended) or to embed a copy of the article.
   - **Show on new record** (Platform Attach actions only): Allows the **Attach** button to be shown while creating a record instead of just appearing on an existing record. Earlier, the ITIL or admin user had to fill out required fields and save the record, then re-expand the search results before the **Attach** buttons were made available.

8. Click **Update** to save and close the Table Configuration record.

9. Add the search results area to the form for the associated table.
   a) Navigate to the relevant form for that table. For example, navigate to **Incident > Open** and open an Incident form.
   b) Configure the form and add **Contextual Search Results** in the location where you want to display the results. For example, you can display the search results immediately after the text field the search is based on or at the bottom of the form.

**Define search fields on a form**

Contextual searches are based on the content entered in selected search fields on forms. You can define multiple search fields for a form, with one field selected as the default.

Search results for the default field appear automatically in the **Agent Assist** section when you open a record. Search results in other associated fields only appear when you type content in those fields.

For example, in the base system the **Short description** is the default search field for the Incident form, so search results based on that field are displayed automatically.
If the **Description** field is also defined as a search field on this form, search results only appear when you type content in that field.

1. Navigate to **Contextual Search > Table Configuration** and open the record.
2. Click **New** in the **Search Fields** related list.
3. Select the field to use and the order for that field.

**Note:** Only text fields can be selected.

4. Right-click the header and select **Save** to save the search field record.
5. Optional: If you have multiple search fields defined for that form, you can click **Set as Default** to select the new field as the default search field.

### Create an email notification for search results

Edit the email notification that is sent when the relevant record is created to include search results.

1. Navigate to Open the Table Configuration form for the table.
2. In the **Email Configurations** related list, click **New**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email notification</td>
<td>Email notification to use. For example, the default incident email notification provided is <strong>Incident opened for me</strong>.</td>
</tr>
<tr>
<td>User</td>
<td>Field identifying the user to receive the email. For example, <strong>Opened by</strong> if the email notification is sent to the user who created the record. This information is used to filter the search results included based on that user's access permissions, ensuring that the recipient can always access the information in the links provided.</td>
</tr>
<tr>
<td>Limit</td>
<td>Maximum number of results the email notification includes.</td>
</tr>
</tbody>
</table>

3. Click **Submit**.
4. Configure the email notification to use the contextual search.
   a) Navigate to System Notification > Email > Notifications.
   b) Open the email notification which will include the contextual search results.
   c) Add the following script to the notification
      Message.$(mail_script:cxs_EmailSearchResults)

Search as different user

When you define contextual search for tables, you can choose to display search results as they
would appear to a different user who performs the search.

For example, an HR administrator may want to display contextual search results, for a user who
made an HR request, to find out why these results did not answer the user’s query.

---

**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.

---

1. Navigate to Contextual Search > Table Configuration.
2. Open a table configuration record.
3. In the **Search as** section of the form, fill in the fields as appropriate.
When enabled, Search As displays the search results that appear for the user defined in the condition.

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 conditions are met:

- 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
  `false`.
Search as configuration fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable search as</td>
<td>Check box use search as functionality.</td>
</tr>
<tr>
<td>Search as field</td>
<td>The field on the table to identify the user to search as. You can only select <strong>User Reference</strong> fields. For example, select <strong>Opened by</strong> to search as the user who opened the relevant record.</td>
</tr>
<tr>
<td>Condition</td>
<td>Specify the conditions based on which the search as results are displayed.</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&quot;)</code>.</td>
</tr>
</tbody>
</table>

**Note:** Both **Condition** and **Script** must evaluate to true for the results to be displayed.

**Note:** An empty script evaluates to true.

When an eligible user opens the form for this table and enters search terms, two tabs are displayed: one with the search results the user sees (**My Results**), and one with the search results the other defined user sees (**<User name>’s results**).

**Note:**
- The **My Results** tab searches using the currently logged in user.
- The **Search as user** tab searches using the **User Reference** field selected by the administrator. For example: the user who made the request (Opened by or Caller fields).
- 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.

**Define contextual search for record producer**

You can define a record producer to trigger a search based on text entered in a variable field. Search results appear at the bottom of the record producer form.

For example, add contextual search to the **Description** variable in the Report an Issue record producer to provide potential answers to users who submit the form.

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**. You can also open a search context and click **New** in the **Record Producer Configurations** related list.

![Record Producer Configuration Form](image)

2. Complete the form.

**Configuration fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record producer</td>
<td>Name of the record producer to add the search to.</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 which uses the contextual search.</td>
</tr>
<tr>
<td>Results header text</td>
<td>Label for the search results area that appears on the record producer.</td>
</tr>
<tr>
<td>Active</td>
<td>Check box for activating this record producer configuration.</td>
</tr>
<tr>
<td>Limit</td>
<td>Maximum number of items to display in the results area. By default, this limit is set to 10. To return an unrestricted number, leave this field blank.</td>
</tr>
<tr>
<td>Results per page</td>
<td>Number of results that are shown per page in the results area.</td>
</tr>
<tr>
<td>Allow expand/collapse</td>
<td>Check box to allow the user to collapse the search results in the form.</td>
</tr>
</tbody>
</table>

3. Open the form context menu and click **Save**.

4. Optional: Refer to the following topics to add a filter configuration.

Filter configurations are defined to map fields from two different tables to provide a more targeted search result set. You can do any of the following:

- [Create a filter configuration using mapping](#)
- [Create a filter configuration using scripting](#)
5. Optional: Modify the search actions that you can perform on the search result.
   The Search Action Configurations related list contains all the available Search Actions available for the selected Search context. Search Actions can be modified but not deleted and new actions cannot be created.

   The Search Actions that can be modified are as follows:
   
   - **Action label**: Display label that is shown on the Action button in result list.
   - **Action value**: Value that is logged into the query feedback table when the action is taken.

6. Click Update to save and close the Record Producer Configuration record.

**Apply configuration to search**

You can apply configurations to define conditions for each search context. For example, you can configure the catalog search resource to only display search results from a specific service catalog.

1. In the **Search Context** form, open the **Resource Configuration** related list to show the resource configurations available for that context. The resource configurations available are based on the searcher selected for this search context.

2. Click the arrow icon beside the searcher name to expand the entry, showing which configuration properties are available.
3. Click a property name to view the property details.

### Search Properties

<table>
<thead>
<tr>
<th>Catalog Search Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalog name</td>
<td>Restrict the search results displayed to those within the named catalog.</td>
</tr>
<tr>
<td>Search operator</td>
<td>Alter how to combine AND and OR conditions when parsing the search string, to score the results displayed. Set this to:</td>
</tr>
<tr>
<td></td>
<td>- <strong>IR_AND_OR_QUERY</strong> (the default): Display results with exact matches of all terms if the number of results is greater than the value of the <code>glide.ts.query.and_or_limit</code> property (default 0) or the (overriding) value of the table custom attribute <code>text_search_and_or_limit</code> (when added). Otherwise display results with any matches of any terms.</td>
</tr>
<tr>
<td></td>
<td>- <strong>IR_AND_QUERY</strong>: Display results with exact matches of all terms only.</td>
</tr>
<tr>
<td></td>
<td>- <strong>IR_OR_QUERY</strong>: Display results with any matches of any terms.</td>
</tr>
</tbody>
</table>
Create a filter configuration using mapping

You can create a simple filter mapped to a table configuration or a record producer configuration to filter the search results.

Role required: admin

Examples:

- Filter to only show knowledge articles for an incident where both are mapped to the same configuration item.
- Filter to only show knowledge articles for a case where both are mapped to the same product.

1. Navigate to **Contextual Search > Table Configuration** or **Record Producer Configuration**.
2. Select a table configuration on which to create the filter (for example, Incident) or select a record producer configuration on which to create the filter (for example, Create Incident).
3. From the Filter Configurations related list, click **New**.
4. Fill in the **Resource configuration** field on the Filter Configuration form with the resource to be searched (for example, knowledge, social, etc.).
5. Ensure that the **Active** check box is selected.
6. Click **Submit**.
7. Open the newly created filter configuration from the Filter Configurations related list.
8. From the Filter Conditions related list, click **New**.
10. Select a **Field to compare** from Query table, and a **Compare to** from Current form or Record producer.

   For example – filter by configuration item:

   

   ```
   Incident (incident):Configuration item = Knowledge (kb_knowledge):Configuration item
   ```

11. Click **Submit**.

Create a filter configuration using scripting

You can create a filter with scripting mapped to a table configuration or a record producer configuration to filter the search results.

Role required: admin

Examples:

- Filter to only show knowledge articles for an incident where both are mapped to the same configuration item.
- Filter to only show knowledge articles for a case where both are mapped to the same product.

1. Navigate to **Contextual Search > Table Configuration** or **Record Producer Configuration**.
2. Select a table configuration on which to create the filter (for example, Incident) or select a record producer configuration on which to create the filter (for example, Create Incident).
3. From the Filter Configurations related list, click **New**.
4. Fill in the **Resource configuration** field on the Filter Configuration form with the resource to be searched (for example, knowledge, social, etc.).
5. Ensure that the **Active** check box is selected.
6. Select the **Scripted filter** check box.
7. Add script content to the Script section to configure the filter.
8. Click **Submit**.

```
(function(current, query_table) {
    /**
     * current: A GlideRecord representing the Form or Record producer
     * query_table: The table to compare value on
     * Use the standard query features of GlideRecord to add conditions to query_table.
     * Current preprepresents the current values on the user's form or record producer that
     * can be used to add live conditions to the query.
     * E.g. query_table.addQuery("active", current.active);
     * The return value should always be the encoded query, usually
     * query_table.getEncodeQuery()
     */

    query_table.addActiveQuery();
    // Return the encoded query
    return query_table.getEncodedQuery();
})(current, query_table);
```

### Contextual search roles

Contextual search involves the following roles.

<table>
<thead>
<tr>
<th>Role title (Name)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator (admin)</td>
<td>Access and use contextual search functions.</td>
</tr>
</tbody>
</table>

### Deflect and resolve incidents with knowledge

Incident deflection and resolution with knowledge provides contextual search results.

Contextual search is provided 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.

You can run feedback reports to track where these search results are marked as helpful.

You must have the admin role to configure contextual search.
Provide knowledge in an incident form

The Incident form displays contextual search results based on text entered in the Short Description field. These search results provide targeted knowledge to the incident analyst.

If the user who raised the incident has indicated that a returned result was useful, the incident analyst can review this information in more detail to help resolve the incident more quickly.
<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>INC0000055</td>
</tr>
<tr>
<td>Caller</td>
<td>Carol Coughlin</td>
</tr>
<tr>
<td>Location</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>-- None --</td>
</tr>
<tr>
<td>Subcategory</td>
<td>-- None --</td>
</tr>
<tr>
<td>Configuration item</td>
<td>SAP Sales and Distri</td>
</tr>
<tr>
<td>Impact</td>
<td>1 - High</td>
</tr>
<tr>
<td>Urgency</td>
<td>1 - High</td>
</tr>
<tr>
<td>Priority</td>
<td>1 - Critical</td>
</tr>
<tr>
<td>Short description</td>
<td>SAP Sales app is not accessible</td>
</tr>
</tbody>
</table>

**Related Search Results**

1. **Can't access SAP**
   - SAP troubleshooting techniques Using transaction SE11, create a table with the same fields as the table in the external database, make sure that...

2. **SAP Outage - We are aware of the SAP out...**
   - SAP Outage - We are aware of the SAP outage. Service will be restored...

3. **How to access office email from a home n...**
   - How to access office email from a home network

4. **Sales Force Automation is DOWN**
   - Sales Force Automation is DOWN
You can configure contextual search functionality to change which fields are searched on or to add contextual search to other forms.

Provide knowledge in incident record producer

Incident deflection provides self-service users with contextual knowledge when they create an incident using either the Create Incident record producer or the Something Broken ESS record producer.

Contextual search results appear based on text entered in the Please describe your issue below field of the Create Incident record producer, or in the Short description field of the Something Broken ESS record producer.

Users can indicate whether a search result is useful to them. If the knowledge provided resolved the incident, the user can cancel the record producer, which deflects the incident. The following scenario shows an example of this.

1. Navigate to the service catalog and select the Can we help you? category.
2. Select the Create New Incident catalog item to raise an incident.
   The Create Incident record producer is displayed.

3. Contextual search then searches the text entered in the Please describe your issue below field to display knowledge results.
4. The user can click an entry in the results list to view the article.
5. The user can then indicate that the article helped, navigate to another article, or close the article.

6. If the knowledge provided helps resolve the issue, the user can cancel the incident record producer. The incident has been deflected. If the information did not fully resolve the issue, the user can still submit the incident.

You can configure contextual search functionality to adapt it to your organization's incident record producers, or to add contextual search to other record producers. For example, customized incident record producers do not have contextual search enabled by default, so you can add contextual search to a customized record producer.

**Provide knowledge in incident email notification**

Contextual search results are included in email notifications that are sent to users who create a new incident. This 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.
For example:

1. Navigate to 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*. For example, one article could be *How to upgrade your Windows version to stop your laptop crashing*.
5. The customer may then be able to use the returned results to resolve the incident.

**Note:**
The knowledge links provided are filtered to ensure the articles are accessible to the user who submitted the email.

By default, notifications provide three article links. You can configure notification options, such as changing the number of links provided with notifications, can be configured by administrators.

You can also configure contextual search functionality to match your organization's email notifications or to use contextual search with notifications for other records.

**Attach an article**

If contextual search is available in a form that uses the knowledge search icon, that icon is removed to ensure there is only a single knowledge search mechanism for that form.

To retain the ability to attach a selected article to that form, an extra **Attach** button appears on the search results list, and an **Attach to incident** button appears on the displayed knowledge article.
Attach Button

Click the relevant button to attach that knowledge article to that incident, adding details of the knowledge article to the task.

Note:
- When you click attach, a note about the KB article is copied or appended to the Additional comments field. Update or save the form or use Post to add the note into the Activity Stream.
- You can also Specify the field a KB article is copied to.

Administer contextual search

You can configure contextual search functions. These procedures require the admin role.
## Contextual Search properties

Navigate to **Contextual Search > Properties** to view and edit contextual search properties.

### Property label (Name) | Description
--- | ---
Default value for maximum number of search results returned for table and record producer configurations (com.snc.contextual_search.result.default.limit) | Set an upper limit on the number of search results displayed in record producers or forms using contextual search. By default, this is set to 10.

Number of milliseconds that a configured field will wait before triggering a search (com.snc.search.service.wait_time) | Set the amount of time after a user finishes typing before running a search based on the typed text. By default, this is set to 500 (half a second).

Records returned above this threshold will log warnings (com.snc.contextual_search.result.threshold) | Trigger a warning message within the system log whenever more than this number of results is returned in a search. This logging helps if you are experiencing performance issues because of large searches. By default, this is set to 10,000.

When a Form configuration is created a search field with a name matching this property will be automatically created (com.snc.contextual_search.widget.form.default_field) | Link the context search to the search field identified in this property whenever you create a new context search for a form. This eliminates the need to select the field in the form manually. By default, this is set to short_description, meaning that whenever you create a new context search for a form with a short_description field, that field is automatically selected as the field the context search acts on.

Collapse the search results widget when opening an existing record in a form (com.snc.contextual_search.widget.form.open_collapsed_existing_records) | When set to true, the search results widget will be collapsed when an existing record is opened. By default, this is set to true.

**Note:** This applies only to existing records and not new records.

Show meta data on form contextual search results (com.snc.contextual_search.widget.form.show_meta_data) | When selected, the search results in the task form displays meta data related to each KB article.

### Run a feedback report

You can report on searches (for example, where a knowledge article was marked as helpful, or attached or a catalog item was ordered) to measure the effectiveness of the contextual search results.

For example, service desk managers can produce a report on user issues that were resolved without an incident being raised to help measure the benefits of incident deflection using knowledge. This information can help to create targeted knowledge based on trends.

For example, analyzing commonly-raised incidents then creating knowledge articles based around those incidents can help resolve or deflect similar incidents in future.

1. Navigate to **Reports > View / Run**.
2. Select the report to run.

Reports available by default are:
- **Number of deflected incidents over the last 3 months**: A line chart displaying the total number of deflected incidents per month for the last 3 months.
- **Successful deflection articles by search term**: A grouped list of search terms and the knowledge articles that were marked as helpful.
- **Top 15 most helpful articles**: A bar chart showing the top 15 articles that have been marked as helpful.

**Note:** You can also run a report by navigating to and searching for the word **Relevant**.

You can create additional feedback information reports by querying feedback tables.

**View a searcher**

Searchers specify where to locate information for a contextual search, such as knowledge and catalog items.

Searcher records are read-only, but you should be aware of the searchers available so you can select the correct one when defining contextual searches.

1. Navigate to **Contextual Search > Searchers**, then open a record.
2. Use the Search Resources related list to inspect the sources which define the information areas to search.
   For example, incident deflection uses the **knowledge and catalog** searcher which includes knowledge and catalog resources.

Search resources can also contain properties, refining the resource further. For example, the knowledge search resource contains a Sort order property to specify that the search results are returned sorted by relevance.
Domain separation and Contextual Search

This is an overview of domain separation with Contextual Search. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can then control several aspects of this separation, including which users can see and access data.

Overview

Support: Level 2

Domain separation is supported in this application. Not all ServiceNow applications support domain separation; some include limitations on the data and administrative settings that can be domain separated. To learn more, see Application support for domain separation.

Contextual searches are enabled for incidents by default, providing incident deflection using knowledge and social Q&A questions. With regard to domain separation, you can search as the currently logged-in user as well as search as a different user. This feature is enabled in separated domains as well.

How domain separation works in Contextual Search

By default, Contextual Search displays results using 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 display 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).

Query feedback information

The information captured when the user clicks the Action button (for example, This helped, Order or Attached) on the result window is stored in the following tables.
Relevant Document (cxs_relevant_doc)

Groups the Relevant Document Detail individual recorded actions by search session.

**Note:** A new search session group is created every time you create or open a record or reload the page.

Key fields in the Relevant Document table:
- **Search session:** The search session group.
- **Displayed on:** The table or record producer where the results were displayed.
- **Relevant to:** The reference to the table record (when displayed on is for a table).
- **User/Created by:** The user who took the action.

Relevant Document Detail (cxs_rel_doc_detail)

The list of individual recorded actions, for example: Preview, This helped, Attach, Order.

Key fields in the Relevant Document table:
- **Search term:** The search text.
- **Original search terms:** The original search terms (only used when the fulfiller has overridden the original search terms using the related search box).
- **Relevance type:** The recorded action.
- **Relevant document:** The result the action was taken on.
- **Relevant Document:** The reference to the search session group in the Relevant Document table.
- **Created by:** The user who took the action.
- **Position:** The position in the list of the result for the recorded action.

This feedback information is important for analyzing the effectiveness of the searches provided. You can create custom reports on this information by querying these tables.

**Installed with contextual search**

Several components are added with activation of the Contextual Search plugin.

**Business rules installed with contextual search**

Contextual search adds the following business rules.

<table>
<thead>
<tr>
<th>Name</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add variable to record producer</td>
<td>Record Producer Configuration (cxs_rp_config)</td>
<td>Contains script that adds contextual search to the selected variable on a record producer.</td>
</tr>
<tr>
<td>Name</td>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Add variable to wizard</td>
<td>Wizard Configuration (cxs_wizard_config)</td>
<td>Contains script that adds contextual search to the selected variable on a wizard.</td>
</tr>
<tr>
<td>Cascading delete for removed config</td>
<td>Table Configuration (cxs_table_config)</td>
<td>Deletes search fields when the related table configuration is deleted.</td>
</tr>
<tr>
<td>Check for duplicate</td>
<td>Table Configuration (cxs_table_config)</td>
<td>Avoids duplicate table configurations.</td>
</tr>
<tr>
<td>Check for duplicate</td>
<td>Email Configuration (cxs_table_email_config)</td>
<td>Avoids duplicate table email configurations.</td>
</tr>
<tr>
<td>Check for duplicate</td>
<td>Wizard Configuration (cxs_wizard_config)</td>
<td>Avoids duplicate wizard configurations.</td>
</tr>
<tr>
<td>Check for duplicate</td>
<td>Record Producer Configuration (cxs_rp_config)</td>
<td>Avoids duplicate record producer configurations.</td>
</tr>
<tr>
<td>Check for invalid action values</td>
<td>Base UI Configuration (cxs_ui_config_base)</td>
<td>Checks for invalid action values against the related search configuration.</td>
</tr>
<tr>
<td>Create default search field</td>
<td>Table Configuration (cxs_table_config)</td>
<td>Creates a default search field when an insert or update is performed on a table configuration.</td>
</tr>
<tr>
<td>Create m2m_kb_task record on attach</td>
<td>Relevant Document Detail (cxs_rel_doc_detail)</td>
<td>Creates a knowledge base task record.</td>
</tr>
<tr>
<td>Delete m2m_kb_task record on remove</td>
<td>Relevant Document Detail (cxs_rel_doc_detail)</td>
<td>Deletes a knowledge base task record.</td>
</tr>
<tr>
<td>Display default context config message</td>
<td>Client Configuration (cxs_client_config)</td>
<td>Confirms the default search context configuration.</td>
</tr>
<tr>
<td>Display default field message</td>
<td>Search Field (cxs_table_field_config)</td>
<td>Confirms the default table field.</td>
</tr>
<tr>
<td>If searcher changes check interleaved</td>
<td>Search Context (cxs_context_config)</td>
<td>Check weather a search context needs to interleaved</td>
</tr>
<tr>
<td>Maintain context resource properties</td>
<td>Search Context (cxs_context_config)</td>
<td>Is used to update context properties</td>
</tr>
<tr>
<td>Make default</td>
<td>Search Context (cxs_context_config)</td>
<td>Sets the client configuration as the default.</td>
</tr>
<tr>
<td>Make default config</td>
<td>Search Field (cxs_table_field_config)</td>
<td>Sets the table field as the default.</td>
</tr>
<tr>
<td>Populate “Order” field</td>
<td>Search Field (cxs_table_field_config)</td>
<td>Sets the order for new search field configurations. Order will be set to the highest order in the list.</td>
</tr>
<tr>
<td>Name</td>
<td>Table Configuration</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Remove related search field records</td>
<td>Table Configuration (cxs_table_config)</td>
<td>Removes related search fields when changes are made to a record producer.</td>
</tr>
<tr>
<td>Remove related search field records</td>
<td>Record Producer Configuration (cxs_rp_config)</td>
<td>Removes related search fields when changes are made to a table.</td>
</tr>
<tr>
<td>Set &quot;Name&quot; field</td>
<td>Record Producer Configuration (cxs_rp_config)</td>
<td>Sets the name of a record automatically for record producers.</td>
</tr>
<tr>
<td>Set &quot;Name&quot; field</td>
<td>Table Configuration (cxs_table_config)</td>
<td>Sets the name of a record automatically for forms.</td>
</tr>
<tr>
<td>Set &quot;Name&quot; field</td>
<td>Email Configuration (cxs_table_email_config)</td>
<td>Sets the name of a record automatically.</td>
</tr>
<tr>
<td>Set &quot;Name&quot; field</td>
<td>Search Field (cxs_table_field_config)</td>
<td>Sets the name of a record automatically.</td>
</tr>
<tr>
<td>Update related context config records</td>
<td>Search Resource (cxs_search_res_config)</td>
<td>Used to update related search context configuration records</td>
</tr>
<tr>
<td>Validate active context</td>
<td>Base UI Configuration (cxs_ui_config_base)</td>
<td>Used to confirm that the search context is valid</td>
</tr>
<tr>
<td>Validate limit</td>
<td>Email Configuration (cxs_table_email_config)</td>
<td>Ensures the limit is not negative or zero for email configurations.</td>
</tr>
<tr>
<td>Validate limit</td>
<td>Record Producer Configuration (cxs_rp_config)</td>
<td>Ensures the limit is not negative or zero for record producer configurations.</td>
</tr>
<tr>
<td>Validate limit</td>
<td>Table Configuration (cxs_table_config)</td>
<td>Ensures the limit is not negative or zero for form configurations.</td>
</tr>
<tr>
<td>Validate results per page</td>
<td>Table Configuration (cxs_table_config)</td>
<td>Ensures the limit is not negative, zero or greater than limit for forms.</td>
</tr>
<tr>
<td>Validate results per page</td>
<td>Record Producer Configuration (cxs_rp_config)</td>
<td>Ensures the limit is not negative, zero or greater than limit for record producers.</td>
</tr>
</tbody>
</table>

**Client scripts installed with contextual search**

Contextual search adds the following client scripts.

**Client scripts installed with contextual search**

<table>
<thead>
<tr>
<th>Name</th>
<th>Table Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set default limit and results per page</td>
<td>Record Producer Configuration (cxs_rp_config)</td>
</tr>
<tr>
<td>Clear field when Record Producer changes</td>
<td>Record Producer Configuration (cxs_rp_config)</td>
</tr>
<tr>
<td>Name</td>
<td>Table</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>Set default limit and results per page</td>
<td>Table Configuration (cxs_table_config)</td>
</tr>
<tr>
<td>Warn about search fields being removed</td>
<td>Table Configuration (cxs_table_config)</td>
</tr>
<tr>
<td>Set default limit</td>
<td>Email Configuration (cxs_table_email_config)</td>
</tr>
<tr>
<td>Set default limit and results per page</td>
<td>Wizard Configuration (cxs_wizard_config)</td>
</tr>
<tr>
<td>Clear field when Wizard changes</td>
<td>Wizard Configuration (cxs_wizard_config)</td>
</tr>
</tbody>
</table>

**Email notifications installed with contextual search**

Contextual search modifies the following email notifications.

<table>
<thead>
<tr>
<th>Name</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident opened for me</td>
<td>Incident (Incident)</td>
<td>Shows the search result records that contextual search finds for that incident record.</td>
</tr>
</tbody>
</table>

**Note:** A note indicates neutral or positive information that emphasizes or supplements important points of the main text. A note supplies information that may apply only in special cases. Examples are memory limitations, equipment configurations, or details that apply to specific versions of a program.

**Script includes installed with contextual search**

Contextual search adds the following script includes.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Extends</th>
</tr>
</thead>
<tbody>
<tr>
<td>cxs_App</td>
<td>Configures business rules, action scripts, and security script against tables using contextual search.</td>
<td>N/A</td>
</tr>
<tr>
<td>cxs_ContextConfig</td>
<td>Configures Table Configuration (cxs_table_config) attributes.</td>
<td>N/A</td>
</tr>
<tr>
<td>cxs_FormatResults</td>
<td>Determines and runs the macro to be used for displaying search results.</td>
<td>N/A</td>
</tr>
<tr>
<td>cxs_Knowledge</td>
<td>Attaches knowledge articles to records such as incidents, change requests, and problems.</td>
<td>AbstractAjaxProcessor</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Extends</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>cxs_RPAjax</td>
<td>Gets and retrieves record producer configurations.</td>
<td>AbstractAjaxProcessor</td>
</tr>
<tr>
<td>cxs_RPCConfig</td>
<td>Configures the Record Producer Configuration (cxs_rp_config) table and manipulates contextual search on record producers.</td>
<td>N/A</td>
</tr>
<tr>
<td>cxs_RPVarTypes</td>
<td>Returns the types of variable that can be used when defining a contextual search for a record producer.</td>
<td>N/A</td>
</tr>
<tr>
<td>cxs_SearchContextAJAX</td>
<td>Configures records in the Search Resource Context Configuration (cxs_res_context_config) table.</td>
<td>AbstractAjaxProcessor</td>
</tr>
<tr>
<td>cxs_SearchResourceConfig</td>
<td>Contains method that will update Context Configuration for (cxs_search_res_config).</td>
<td>N/A</td>
</tr>
<tr>
<td>cxs_SearchResultsAJAX</td>
<td>Returns results from a search formatted using the specified macro.</td>
<td>AbstractAjaxProcessor</td>
</tr>
<tr>
<td>cxs_SearchServerAJAX</td>
<td>Checks that the search context is configured.</td>
<td>AbstractAjaxProcessor</td>
</tr>
<tr>
<td>cxs_TableActions</td>
<td>Gets email search request records.</td>
<td>N/A</td>
</tr>
<tr>
<td>cxs_TableAjax</td>
<td>Gets table configuration from the Table Configuration (cxs_table_config) table.</td>
<td>AbstractAjaxProcessor</td>
</tr>
<tr>
<td>cxs_TableConfig</td>
<td>Creates and configures fields that have contextual search attached from the (cxs_table_field_config) table.</td>
<td>N/A</td>
</tr>
<tr>
<td>cxs_TableEmailConfig</td>
<td>Configures and checks duplicates in the Email Configuration (cxs_table_email_config) table.</td>
<td>N/A</td>
</tr>
<tr>
<td>cxs_TableEmailConfigAJAX</td>
<td>Configures the Email Configuration (cxs_table_email_config) table.</td>
<td>AbstractAjaxProcessor</td>
</tr>
<tr>
<td>cxs_TableFieldConfig</td>
<td>Configures records in the Search Field (cxs_table_field_config) table.</td>
<td>N/A</td>
</tr>
<tr>
<td>cxs_TableFieldTypes</td>
<td>Used to validate field types.</td>
<td>Search Field (cxs_table_field_config) table.</td>
</tr>
<tr>
<td>cxs_WizardAJAX</td>
<td>Gets and retrieves wizard configuration.</td>
<td>AbstractAjaxProcessor</td>
</tr>
<tr>
<td>cxs_WizardConfig</td>
<td>Creates and configures fields that have contextual search attached.</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Tables installed with contextual search

Contextual search adds or modifies the following tables.

<table>
<thead>
<tr>
<th>Display Name (Table Name)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available Search Resource (v_cxs_search_resource)</td>
<td>A virtual table that contains a list of available search resources used in configuration of searches.</td>
</tr>
<tr>
<td>Email Configuration (cxs_table_email_config)</td>
<td>Contains a list of email notifications configured to have contextual search results attached.</td>
</tr>
<tr>
<td>Record Producer Configuration (cxs_rp_config)</td>
<td>Contains a list of record producers configured to have contextual search.</td>
</tr>
</tbody>
</table>
| Relevant Document (cxs_relevant_doc) | Contains incident record references where users have indicated that a search result record was useful by clicking the **This helped** button. Significant fields include:  
  - **Displayed on**: Whether the contextual search results were shown on a table form or a record producer.  
  - **Session id**: The id of the search session that the action button was triggered for.  
  - **Helped with**: The record that the search result helped resolve. |
| Relevant Document Detail (cxs_rel_doc_detail) | Contains all the search result records which users have indicated were useful or have attached to a form, as well as the search terms used in the search query. Significant fields include:  
  - **Relevance**: The internal value of the action button (**This helped** or **Attach**).  
  - **Help document**: The search result that was marked as helped or attached.  
  - **Help document URL**: The URL to the article that was marked as helped or attached.  
  - **Search request**: The JSON object that was used by the search engine to perform the search.  
  - **Search term**: The search term that was used to initiate the search. |
| Search Context (cxs_context_config) | Contains available search contexts for contextual search. |
| Search Field (cxs_table_field_config) | Contains all form fields which have contextual search configured to it. |
| Search Resource (cxs_search_res_config) | Contains search resource configurations for the related searcher. |
### Display Name (Table Name) | Description
---|---
Search Resource Context Configuration (cxs_res_context_config) | Contains conditions for this search context that will restrict the results returned to a user.
Search Resource Context Property (cxs_res_context_config_prop) | Contains the property values for search resource context configuration.
Search Resource Property (cxs_search_res_config_prop) | Contains the property values for search resource searcher configuration.
Searcher Configuration (cxs_searcher_config) | Contains the details of available search configurations.
Table Configuration (cxs_table_config) | Lists the tables configured for table configurations.
Wizard Configuration (cxs_wizard_config) | Lists the tables configured for wizard configurations.
Base UI Configuration (cxs_ui_config_base) | Contains the common elements for the record producer, table, and wizard configurations.

#### UI macros installed with contextual search

Contextual search adds the following UI macros.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cxrResult</td>
<td>Represents a single search result when processed by cxrResults.</td>
</tr>
<tr>
<td>cxrResults</td>
<td>Processes the results returned by a contextual search.</td>
</tr>
<tr>
<td>cxrResultsHeaderEmail</td>
<td>Adds the header when sending contextual search results by email.</td>
</tr>
<tr>
<td>cxrResultsHeaderRp</td>
<td>Displays the header that is shown above the search results on record producers.</td>
</tr>
<tr>
<td>cxrResultsHeaderTable</td>
<td>Displays the header that is shown above the search results on forms.</td>
</tr>
<tr>
<td>cxrResultsHeaderWizard</td>
<td>Displays the header that is shown above the search results wizards.</td>
</tr>
<tr>
<td>cxrResultsTable</td>
<td>Processes the results returned by a contextual search.</td>
</tr>
<tr>
<td>cxrResultsVCR</td>
<td>Provides the pagination controls.</td>
</tr>
<tr>
<td>cxrResultDefault</td>
<td>Represents a single search result where there is no specific macro for the source table.</td>
</tr>
<tr>
<td>cxrResultEmail</td>
<td>Represents a single search result when the search results are being sent by email.</td>
</tr>
<tr>
<td>cxrResultKbKnowledge</td>
<td>Represents a single search result returned from the kb_knowledge table.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>cxs_result_sc_cat_item</td>
<td>Represents a single search result returned from the sc_cat_item table.</td>
</tr>
<tr>
<td>cxs_result_table</td>
<td>Represents a single search result for displaying on a form.</td>
</tr>
<tr>
<td>cxs_rp_search</td>
<td>Initiates a contextual search from a record producer.</td>
</tr>
<tr>
<td>cxs_table_search</td>
<td>Initiates a contextual search from a form.</td>
</tr>
<tr>
<td>cxs_wizard_search</td>
<td>Initiates a contextual search from a record producer.</td>
</tr>
</tbody>
</table>

**UI policies installed with contextual search**

Contextual search adds the following UI policies.

**UI Policies installed with contextual search**

<table>
<thead>
<tr>
<th>UI Policy</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hide Table field</td>
<td>Email Configuration</td>
<td>Changes email configuration visibility to false and read only.</td>
</tr>
<tr>
<td></td>
<td>(cxs_table_email_config)</td>
<td></td>
</tr>
<tr>
<td>Hide table config field</td>
<td>Search Field</td>
<td>Hides the table field on the form.</td>
</tr>
<tr>
<td></td>
<td>(cxs_table_field_config)</td>
<td></td>
</tr>
</tbody>
</table>

**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 (sys_event) 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:

**Event fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The unique name of event. Baseline event names include the record effected and the triggering action such as incident.commented.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Parm1</td>
<td>An 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>
<tr>
<td>Parm2</td>
<td>Another 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>
<tr>
<td>Table</td>
<td>The table to which the event applies. This is the same table on which the business rule ran.</td>
</tr>
<tr>
<td>Instance</td>
<td>The Sys ID of the record to which this event applies.</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.

**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>State</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------------</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>
<tr>
<td>Transferred</td>
<td>The event was rotated to a different shard of the Event (sys_event) table. When an event is rotated, a duplicate record is created in an active shard to be processed. A scheduled job processes the event when it is next in the queue, but it is not possible to predict when this will happen as because several events may need to be processed before it. Therefore, you can reprocess the event. See Reprocess an event.</td>
</tr>
</tbody>
</table>

Event logs

The event log records all system events that occur within the system. 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>

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') {
    gs.eventQueue("incident.inserted", current, gs.getUserID(), gs.getUserName());
}
```

```
if (current.operation() == 'update') {
    gs.eventQueue("incident.updated", current, gs.getUserID(), gs.getUserName());
}
```

```
if ((current.assignee_to.nil()) && current.assignee_to.changes()) {
    gs.eventQueue("incident.assignee", current, current.assignee_to.getDisplayValue(), previous.assignee);
}
```

```
if ((current.assignment_group.nil()) && current.assignment_group.changes()) {
    gs.eventQueue("incident.assignment_group", current, current.assignment_group.getDisplayValue(), previous.assignment_group);
}
```
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')
```

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 true. Usually this is expressed as current, 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 parm1 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 parm2 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());
}
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 (!current.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 configuration 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</td>
</tr>
<tr>
<td></td>
<td>your script action that suits your purpose, you can create a new one.</td>
</tr>
<tr>
<td>Application</td>
<td>The application that contains this script.</td>
</tr>
<tr>
<td>Field</td>
<td>Input Value</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</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 Script 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:</td>
</tr>
<tr>
<td></td>
<td>- event: a - 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.</td>
</tr>
<tr>
<td></td>
<td>- current: a GlideRecord - the event scheduled on behalf of (incident for example).</td>
</tr>
</tbody>
</table>

This is a sample of a script action that creates an email notification for Workflow activity:
```
/*
  * Handle a workflow.notification event by creating an email notification that can be sent
  * param1 - sys_id of workflow activity, sys_id of workflow context
  * param2 - comma-separated list of recipients
  */

function sendWorkflowNotification() {
  // get the activity that defines the information about the event
  var activity = new GlideRecord('wf_activity');
  if (activity.get(parts[0]))
    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 == 2)
    context.get(parts[1]);
  GlideController.putGlobal("context", context);
  var workflow = new Workflow().newWorkflowProxy();
  GlideController.putGlobal("workflow", workflow);

  var subject = new GlideWorkflowActivity vars.subject();
  var message = new GlideWorkflowActivity vars.email();
  var emailAction = new GlideEmailAction();
  var emailGR = new GlideRecord('sys/event_email_action');
  */
```

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_requestCOMMENTED`
- `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.

   ```java
   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.

```javascript
(function executeRule(current, previous /*null when async*/) {
    //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. Complete the Event Registration form as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Input Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of your new event.</td>
</tr>
<tr>
<td>Table</td>
<td>The database table for this event.</td>
</tr>
<tr>
<td>Description</td>
<td>Short description of the purpose of the event.</td>
</tr>
</tbody>
</table>

*Note: The list shows only tables and database views that are in the same scope as the event.*
### 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 gr = new GlideRecord('sc_req_item');
   gr.get('sys_id', id);
   if (gr.next()){
     // Do something.
   }
   ```
Data management

Data in your instance is stored and managed 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 table has all of the 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 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 **MatchField** field represents a Date/Time column in the table that you are trying to clean up.
- The **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.

**Note:** TableCleaner does not call DBDelete.setWorkflow(). 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>Table</td>
<td>Tracked field</td>
<td>Time to deletion</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------</td>
<td>------------------</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><strong>Data Archiving</strong></td>
<td>Provides the ability to archive records to minimize performance issues.</td>
</tr>
<tr>
<td><strong>Database Rotations</strong></td>
<td>Provides tools for managing large tables to minimize performance issues.</td>
</tr>
<tr>
<td><strong>Many to Many task relations</strong></td>
<td>Provides the ability to define many-to-many relationships between task tables.</td>
</tr>
</tbody>
</table>

**The unique record identifier (sys_id)**

Each record in the instance is identified by a unique 32-character GUID (Globally Unique ID) called a Sys ID (sys_id). There are various ways to obtain the sys_id of a record.

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, then one was copied to the other at the database level outside of the Now Platform. When created within the application, sys_id values are unique. The Now Platform and database should manage all operations on sys_id values.

**Note:** A sys_id of -1 is the sys_id of a new record. Once the record is inserted, it will be given a new sys_id.

**Note:** 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 Hi 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.

   ```
   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

The archive application moves data that is no longer necessary for immediate day-to-day access from primary tables into a set of archive tables.

The longer an instance runs, the more likely it is to accumulate data that is no longer relevant to current business needs. 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, set up an archive rule to archive the data and remove it from immediate access to free up system resources. You can then set up a destroy rule to delete the data after a specified period of time. Destroy rules are available starting with the Helsinki release.

Sample Benefits of Archiving Data

Data archiving supports Domain separation. For example, incidents that belong to a domain keep their domain designation even after they are archived.

Note: If you want to archive email, 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].
- 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 [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

Querying 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 ServiceNow does not recommend making ad hoc 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.

Activate data archiving

The Data Archiving plugin installs the System Archiving application.
Role required: admin

1. Navigate to System Definition > Plugins.
2. Find and click the plugin name.
3. On the System Plugin form, review the plugin details and then click the Activate/Upgrade related link.
   
   If the plugin depends on other plugins, these plugins are listed along with their activation status.

   If the plugin has optional features that depend on other plugins, those plugins are listed under Some files will not be loaded because these plugins are inactive. The optional features are not installed until the listed plugins are installed (before or after the installation of the current plugin).

4. Optional: If available, 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 practice when you first activate the plugin on a development or test instance.

   You can also load demo data after the plugin is activated by clicking the Load Demo Data Only related link on the System Plugin form.

5. Click Activate.

Set archive rule processing behavior

In order to prevent the archive process from consuming too many system resources, the instance uses several system properties to control how many records the archive rule processes at one interval.

By default an archive rule follows these processing rules:

- Archives 100 records for each batch job
- Sleeps 1 second between batch jobs
- Runs 10 batch jobs in an archive run (every hour)

You can change these default settings by adding the following system properties.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.db.archive.batch_size</td>
<td>Controls how many records an archive rule processes per batch job.</td>
<td>Integer</td>
<td>100</td>
</tr>
<tr>
<td>glide.db.archive.sleep_time</td>
<td>Controls sleep time between each archive rule batch job run, in seconds.</td>
<td>Integer</td>
<td>1</td>
</tr>
<tr>
<td>glide.db.archive.max_iterations</td>
<td>Controls the maximum number of batch jobs to run within an hour.</td>
<td>Integer</td>
<td>10</td>
</tr>
</tbody>
</table>
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 email, 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**.

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>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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. ServiceNow recommends leaving 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>
</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.

<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>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>Action</td>
<td>Select the action you want the archive rule to take on related records. Choices include:</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 longer references the archived record and does not appear as a related 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 Reference 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 Problem ID field in the Incident table that references the related problem records.</td>
</tr>
<tr>
<td></td>
<td>- The Archive action archives the related record in addition to the primary record. For example, if you select the Problem in Incident reference, the related record rule also archives any incident record that references an archived problem.</td>
</tr>
<tr>
<td></td>
<td>- The Clear action removes the reference to the primary record. For example, if you select the Problem in Incident 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 Delete action deletes any record that references the primary record. For example, if you select the Problem in Incident 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 Document ID field which might point to the archived table. For example, if you are archiving problem records, there is a sys ID 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 Archive action updates the Document ID of the related record to point to the archived table. For example, if you select the Table sys ID Attachment(sys_attachment)* reference, the related record rule updates the attachment record to change the Document ID to refer to the archived table record.</td>
</tr>
<tr>
<td></td>
<td>- The Clear action updates the Document ID of the related record to point to the archived table.</td>
</tr>
<tr>
<td></td>
<td>- The Delete action deletes any record that references the primary record. For example, if you select the Table sys ID Attachment(sys_attachment)* reference, the related record rule deletes any attachment record that references the archived primary record.</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 Document ID 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 after a specified amount of time.

Role required: admin

1. Navigate to System Archiving > Archive Destroy Rules.
2. Click New.
3. Fill out the form fields (see table).
4. Click Submit.

<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>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>

5. You can check the archive destroy log at any time
**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 Attachment**.
3. Click a record from the archived table to see the archived record.
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 data

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.

Role required: admin

1. Navigate to System Archiving > Archive Log.
2. Select the archived record to restore.
3. Click the **Restore Record** related link.

**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**

Archive rules will not archive restored records. In order to archive a restored record you must manually archive the record.
Role required: admin

1. Navigate to the restored record.
2. Click the Archive Record link.

Export and import XML files

To occasionally migrate data from one instance to another, you can export the 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 since 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

<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>
<tr>
<td>Excel</td>
<td>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.</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.
### Export format

<table>
<thead>
<tr>
<th>Export format</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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>
<tr>
<td>PDF</td>
<td>glide.pdf.max_rows</td>
<td>N/A</td>
<td>1,000</td>
</tr>
</tbody>
</table>

**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.
## Export Limit Examples

<table>
<thead>
<tr>
<th>Example</th>
<th>Property</th>
<th>Table</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exporting to CSV</td>
<td>• glide.csv.export.limit = 20,000</td>
<td>Exporting to CSV</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• glide.ui.export.limit = 10,000</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• com.glide.processors.X = 20,000</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Default export limit for CSV = 10,000</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Exporting to Excel (XLSX)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• glide.xlsx.export.limit = no entry</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• glide.ui.export.limit = no entry</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Default export limit for Excel (XLSX) = 10,000</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Exporting to PDF

<table>
<thead>
<tr>
<th>Example</th>
<th>Property</th>
<th>Table</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exporting to PDF</td>
<td>• glide.pdf.max_rows = 1,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Default export limit for PDF = 1,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Maximum export limit for PDF = 5,000</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Records to be Exported</th>
<th>Records Returned</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,000</td>
<td>1,000</td>
</tr>
<tr>
<td>5,000</td>
<td>1,000</td>
</tr>
</tbody>
</table>

In the first export, all records are returned because the number of records specified for export does not exceed the `glide.pdf.max_rows` property. In the second export, the number of records returned is limited because the number of records specified for export exceeds the default value in the `glide.pdf.max_rows` property.

### 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:

#### 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

You can export a 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.

Note: When exporting PDF data from a form, only the fields that are visible from the current view are exported, with the exception of formatter elements. When exporting XML data, however, all 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.
Export from a v2 list

**Note:** To export records in an embedded list, export the record containing the list.

Export formats include:

- Excel
- CSV
- XML
- 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.</td>
</tr>
<tr>
<td></td>
<td>See Field types affected by export controls for more information.</td>
</tr>
<tr>
<td>Query parameter</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-----------------------------------------------------------------------------</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:

```plaintext
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>INC00000050</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 Loa</td>
</tr>
<tr>
<td>INC00000059</td>
<td>2016-08-10 09:14:39</td>
<td>Unable to access team file share</td>
<td>Rick Berge</td>
<td>New</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INC00000058</td>
<td>2016-08-10 09:37:45</td>
<td>Performance problems with email</td>
<td>Bow Rugeri</td>
<td>New</td>
<td></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></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:

```plaintext
sysparm_display_value = false
```

<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>INC00000050</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 Loa</td>
</tr>
<tr>
<td>INC00000059</td>
<td>2016-08-10 09:14:39</td>
<td>Unable to access team file share</td>
<td>Rick Berge</td>
<td>New</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INC00000058</td>
<td>2016-08-10 09:37:45</td>
<td>Performance problems with email</td>
<td>Bow Rugeri</td>
<td>New</td>
<td></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></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>

**displayvalue**

Example:

```plaintext
displayvalue = true
```
Example:

displayvalue = false

Example:

displayvalue = All
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.
### Export Set Field

<table>
<thead>
<tr>
<th>Column headers</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></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>

<table>
<thead>
<tr>
<th>Column values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exports the display value (Use display value) or raw value (Use raw value) for the CSV, Excel, JSON, XLSX, and XML file formats.</td>
<td></td>
</tr>
</tbody>
</table>

See [Field types affected by export controls](#) for more information.

---

#### Column headers

**Example:**

**Use field label**

<table>
<thead>
<tr>
<th>Number</th>
<th>Opened</th>
<th>Short description</th>
<th>Caller</th>
<th>State</th>
<th>Assignment</th>
<th>Assigned to</th>
</tr>
</thead>
<tbody>
<tr>
<td>INC0000060</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 Loa</td>
</tr>
<tr>
<td>INC0000059</td>
<td>2016-08-10 09:14:29</td>
<td>Unable to access team file share</td>
<td>Rick Bercle</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 Ruggeri</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>2017-09-20 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 field name**

<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>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 Loa</td>
</tr>
<tr>
<td>INC0000059</td>
<td>2016-08-10 09:14:29</td>
<td>Unable to access team file share</td>
<td>Rick Bercle</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 Ruggeri</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>2017-09-20 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</th>
<th>Assigned to</th>
</tr>
</thead>
<tbody>
<tr>
<td>INC0000060</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 Loa</td>
</tr>
<tr>
<td>INC0000059</td>
<td>2016-08-10 09:14:29</td>
<td>Unable to access team file share</td>
<td>Rick Bercle</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 Ruggeri</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>2017-09-20 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**
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>
</tr>
</thead>
<tbody>
<tr>
<td>CSV</td>
<td>glide.export.csv.raw.value</td>
<td>false</td>
</tr>
<tr>
<td></td>
<td>glide.export.csv.column_header_label</td>
<td>false</td>
</tr>
<tr>
<td>Excel</td>
<td>glide.export.excel.display_value</td>
<td>true</td>
</tr>
<tr>
<td></td>
<td>glide.export.excel.column_header_label</td>
<td>true</td>
</tr>
<tr>
<td>JSON</td>
<td>glide.json.return_displayValue</td>
<td>false</td>
</tr>
<tr>
<td>XLSX</td>
<td>glide.export.xlsx.display_value</td>
<td>true</td>
</tr>
<tr>
<td></td>
<td>glide.export.xlsx.column_header_label</td>
<td>true</td>
</tr>
</tbody>
</table>

**CSV**

Example:

`glide.export.csv.raw.value = false` (default)

`glide.export.csv.column_header_label = false` (default)

<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>INC00000010</td>
<td>12/12/15 7:19</td>
<td>Unable to connect to email</td>
<td>Joe Employee</td>
<td>Closed</td>
<td>Network</td>
<td>David Los</td>
</tr>
<tr>
<td>INC00000059</td>
<td>8/10/19 5:14</td>
<td>Unable to access team file share</td>
<td>Rick Brewer</td>
<td>New</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INC00000058</td>
<td>8/10/19 5:37</td>
<td>Performance problems with email</td>
<td>Bob Burger</td>
<td>New</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INC00000057</td>
<td>8/10/19 5:14</td>
<td>Performance problems with wifi</td>
<td>Bertyle Lubby</td>
<td>New</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INC00000055</td>
<td>9/20/17 7:14</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:

`glide.export.csv.raw.value = true`

`glide.export.csv.column_header_label = true`
Excel

Example:

```
glide.export.excel.display_value = true (default)
glide.export.excel.column_header_label = true (default)
```

<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>INC00000000</td>
<td>12/12/16 15:19</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>INC00000009</td>
<td>8/10/16 10:14</td>
<td>Unable to access team file share</td>
<td>Rick Berzle</td>
<td>New</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INC00000008</td>
<td>8/10/16 16:37</td>
<td>Performance problems with email</td>
<td>Bow Rugger</td>
<td>New</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INC00000007</td>
<td>8/10/16 10:06</td>
<td>Performance problems with wifi</td>
<td>Bertie Luby</td>
<td>New</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INC00000005</td>
<td>2017-09-20 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:

```
glide.export.excel.display_value = false
glide.export.excel.column_header_label = false
```

<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>INC00000000</td>
<td>12/12/16 15:19</td>
<td>Unable to connect to email</td>
<td>581cc9d5a05f4005a64f8e4d57c7</td>
<td>Closed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INC00000009</td>
<td>8/10/16 10:14</td>
<td>Unable to access team file share</td>
<td>317f351cc611227c0000b83c2c9b0d3c6</td>
<td>New</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INC00000008</td>
<td>8/10/16 16:37</td>
<td>Performance problems with email</td>
<td>76a82d2c61127d91a658c15f8dab9d41</td>
<td>New</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INC00000007</td>
<td>8/10/16 10:06</td>
<td>Performance problems with wifi</td>
<td>76a82d2c61127d91a658c15f8dab9d41</td>
<td>New</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INC00000005</td>
<td>2017-09-21 21:47</td>
<td>SAP Sales app is not accessible</td>
<td>41c1275f45ef518d00b73f76ebe2</td>
<td>In Progress</td>
<td>Service Desk</td>
<td>Beth Anglin</td>
</tr>
</tbody>
</table>

JSON

Example:

```
glide.json.return_displayValue = false (default)
```

```
"records":
[  {
    "parent": "", "made_sla": "false", "caused_by": "", "watch_list": "", "upon_reject": "", "sys_updated_on": "2017-10-11 20:16:07", "child_incident": "", "hold_reason": "", "approval_history": "", "number": "INC0000001", "resolved_by": "6816f79cc08b9e1c051533b4ac1e441", "sys_updated_by": "admin", "opened_by": "6816f79cc08b9e1c051533b4ac1e441", "user_input": "", "sys_created_on": "2016-02-10"
  }
]
```

Example:

```
glide.json.return_displayValue = true
```
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 glide.excel.use_user_date_format set, otherwise system format.</td>
<td>Excel/XLSX: UTC timezone date/time with user format if glide.excel.use_user_date_format 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 glide.excel.use_user_date_format set, otherwise system format.</td>
<td>Excel/XLSX: Date with user format if glide.excel.use_user_date_format set, otherwise system format.</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>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 glide.excel.use_user_date_format set, otherwise system format.</td>
<td>Excel/XLSX: UTC time, assuming 1970-01-01 as the date with user format if glide.excel.use_user_date_format 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>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 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><code>sysparm_query=(column name) (operator)(value)</code></td>
<td>Displays a list of records that match the query. For example: 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><code>sysparm_orderby=(column name)</code></td>
<td>Sorts a list of records by the column name provided. For example: https://&lt;instance name&gt;.service-now.com/ incident_list.do?XML&amp;sysparm_query=priority=1&amp;sysparm_orderby=assigned_to</td>
</tr>
</tbody>
</table>

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`.

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>https://&lt;instance name&gt;.service-now.com/incident_list.do?CSV&amp;sysparm_orderby=sys_id</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 `b4aedb520a0a0b1001af10e278657d27`. Use the syntax shown in this query to export the next set of records.

   ```
   https://<instance name>.service-now.com/syslog_list.do?XML&sysparm_query=sys_id%3E%3Db4aedb520a0a0b1001af10e278657d27&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.

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 (🔒) 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.

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.
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.

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).

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>
<tr>
<td>Select No and select a table to export data from.</td>
<td>Use this configuration if you have not created an export definition record. A new export definition record is created automatically using the selected table that includes fields from the default list view for that table. You can modify the export definition record as needed after creating the export set.</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>
<tr>
<td>File Path</td>
<td>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.</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.

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><strong>Name</strong></td>
<td>Enter a descriptive name for this scheduled export.</td>
</tr>
<tr>
<td><strong>Export set</strong></td>
<td>Select the export set to schedule.</td>
</tr>
<tr>
<td><strong>Run as</strong></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><strong>Run</strong></td>
<td>Select the frequency for scheduled export.</td>
</tr>
<tr>
<td><strong>Day</strong></td>
<td>Select which day of the week or month to run this scheduled export on. This field appears when the Run field is set to Weekly or Monthly.</td>
</tr>
<tr>
<td><strong>Repeat interval</strong></td>
<td>Enter the number of days and hours to wait before repeating this scheduled export. This field appears when the Run field is set to Periodically.</td>
</tr>
<tr>
<td><strong>Time</strong></td>
<td>Enter the time of day to run the scheduled export.</td>
</tr>
<tr>
<td><strong>Delta Exports</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Enable delta exports</strong></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>
<tr>
<td><strong>Delta on or after</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

_**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._

<p>| <strong>Last export scheduled run</strong> | 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. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conditional</td>
<td>Select this check box to run the schedule only when a condition is met.</td>
</tr>
<tr>
<td>Condition</td>
<td>Write the script to be used to evaluate whether the export should run. This field is visible if you select the Conditional check box.</td>
</tr>
<tr>
<td>Execute pre-export script</td>
<td>Select this check box to run a script before the export begins.</td>
</tr>
<tr>
<td>Pre script</td>
<td>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.</td>
</tr>
<tr>
<td>Execute post-export script</td>
<td>Select this check box to run a script after the export finishes.</td>
</tr>
<tr>
<td>Post script</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 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:

```
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 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 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>
<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>
</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.

<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 London
- Import Sets key concepts

Set up

- Create a data source
- Create a transform map

Administer

- Import Sets properties
- Troubleshoot import set performance

Use

- Run an import
- Importing Data into ServiceNow
- Schedule a data import
- Easy import

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
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:** Data should not be imported 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 will skip records when the data in the instance matches the data being imported.

**Note:** Import Sets run as user System. Therefore, Import Sets 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 prior to transforming those records. Fields on these tables are generated automatically based on imported data and should not be modified manually.</td>
</tr>
<tr>
<td>Data source</td>
<td>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.</td>
</tr>
<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>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------</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>
</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>
<tr>
<td>JSON</td>
<td>• 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.</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>Some network configurations may require a MID Server.</td>
</tr>
<tr>
<td>LDAP</td>
<td>LDAP imports require a valid transform map.</td>
</tr>
</tbody>
</table>

**Import set scheduled cleanup**

The Import Set Deleter scheduled job cleans up old import set data every day at midnight.
By default, the job will delete all import sets that are older than 7 days and 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 that 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 ServiceNow Technical Support to coordinate the deletion of this data.

---

**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. ServiceNow Technical Supports Oracle, MySQL, Sybase, DB2 Universal, and MS SQL Server drivers.</td>
</tr>
</tbody>
</table>
### LDAP

Data is in an LDAP server, accessible through the LDAP or LDAPS ports, 389 and 636 respectively.

### File type data sources

You can 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, including FTP, FTPS, SCP, and HTTPS.

**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. Refer to the following article for an explanation of FTP protocol support [http://en.wikipedia.org/wiki/FTPS](http://en.wikipedia.org/wiki/FTPS).

#### File Retrieval Methods

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attachment</td>
<td><em>Attach</em> a file to the record and import that file in an import set.</td>
</tr>
<tr>
<td>SFTP</td>
<td>Retrieve a file using <em>SFTP</em>. Fields are provided for the server name and login credentials.</td>
</tr>
<tr>
<td>FTP</td>
<td>Retrieve a file from an <em>FTP</em> server in your network. Fields are provided for the server name and login credentials.</td>
</tr>
</tbody>
</table>

**Note:** FTP transfers are sent as clear text and cannot be encrypted. Use SCP or SFTP instead whenever possible.

| FTPS (Auth SSL) (not recommended) | 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. |

---

© 2019 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>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
<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>

**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.

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
<?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>Jerrod</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"
```
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.

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"
    },
    {
      "number":"INC0000002",
    
```
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.

```
{
    "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.

```
{
    "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.

<table>
<thead>
<tr>
<th>Path</th>
<th>Discard Arrays Enabled</th>
<th>Discard Arrays Disabled</th>
</tr>
</thead>
</table>
| /response/docs/docs | Creates one record with the following columns and values:  
- Id : id_val  
- elementWithArray : {} | Creates one record with the following columns and values:  
- Id : id_val  
- childrenArray : (1, 2, 3)  
- anotherArray : ("key1": "value1"), ("key1": "value2")  
- elementWithArray : ("childrenArray" : (1, 2, 3)) |
| /response/docs/docs/anotherArray/anotherArray | Creates two records, each with one column: key1. | Creates two records, each with one column: key1. |
| /response/docs/docs/childrenArray/childrenArray | 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. | 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. |

Orphan array

**Important**: This format is not supported. A JSON array must always be inside an element. The JSON file must always start with { and end with }.

```json
[
  {
    "number":"PRBTEST001",
```
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":"testsd1"
    },
    "problem":{
      "number":"PRBTEST002",
      "short_description":"testsd2"
    }
  },
  "problems":{
    "title":"1 problem",
    "problem":{
      "number":"PRBTEST005",
      "short_description":"testsd5"
    }
  }
}
```

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 name</th>
<th>Description</th>
<th>Default value</th>
<th>Example custom value</th>
<th>Data Source</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>
<td>10000</td>
<td>connection.timeout=12000</td>
<td>FTP, FTPS</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`.

```
SELECT DISTINCT 'server_name:' + CONVERT ( VARCHAR , lg .ResourceID ) AS 'ServerID'
,LastHWScan
,Account0
,Category0
Fromv_GS_WORKSTATION_STATUSsInner JOIN
v_GS_LocalGroupMembers0lg
ON s .ResourceID = lg .ResourceID
```
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

**SCCM 2012 v2 Processor**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>SCCM 2012 v2 Processor</td>
</tr>
<tr>
<td>Import set table label</td>
<td>SCCM 2012v2 Processor</td>
</tr>
<tr>
<td>Import set table name</td>
<td>imp_sccm2012v2_processor</td>
</tr>
<tr>
<td>Type</td>
<td>JDBC</td>
</tr>
<tr>
<td>Use MID Server</td>
<td>Boomer1</td>
</tr>
<tr>
<td>Format</td>
<td>SQLServer</td>
</tr>
<tr>
<td>Instance name</td>
<td></td>
</tr>
<tr>
<td>Database name</td>
<td>testSQL</td>
</tr>
<tr>
<td>Database port</td>
<td></td>
</tr>
</tbody>
</table>

**Related Links**

- Test Load 20 Records
- Load All Records
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.
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.ncri.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.
An LDAP data source is automatically created when you configure your instance to integrate with LDAP.

```
jdbc:teradata://gwhost:port/dbhost
```
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=*)))
```
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).
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.

**Using multiple transform maps**

Multiple transform maps can be applied to a single data source.

One import set row is created per transform map. This behavior 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.
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:

```javascript
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:

```javascript
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_transform"){
   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_transform"){
   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:**

```javascript
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 varname = source.u_name;
var var version = source.u_version;
var 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 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.

var operating_system = source.u_operating_system.toString();

//This if statement uses JavaScript regular expressions to search the operating system  
if( operating_system.match(/linux/i)!=null){  
target.sys_class_name="cmdb_ci_linux_server";};

if( operating_system.match(/win/i)!=null){  
target.sys_class_name="cmdb_ci_win_server";};

User import data sanitation

An example script demonstrating how to sanitize user data before import.

//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>

---

© 2019 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.
Event name | Event Parameters
---|---
onComplete | 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, "");
```
<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>Map of only 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...</td>
</tr>
</tbody>
</table>

© 2019 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>Event name</th>
<th>Event Parameters</th>
</tr>
</thead>
<tbody>
<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>
</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 “insert” or “update” 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 <code>&lt;status_message&gt;</code> XML response.</td>
</tr>
<tr>
<td>Event name</td>
<td>Event Parameters</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>onForeignInsert</td>
<td>When: The onForeignInsert event script is processed at the start of the creation of a related, referenced record, before the record is created.</td>
<td></td>
</tr>
</tbody>
</table>

**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 for which a foreign record is about to be created.</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...</td>
</tr>
<tr>
<td>Event name</td>
<td>Event Parameters</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>------------------</td>
<td></td>
</tr>
<tr>
<td>onReject</td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

**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();
```
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 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 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
gr.query();
if(gr.next())
{
    answer = gr.sys_id; //if a match exists, return the sys_id of the matching User record
}
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>Field</td>
<td>Description</td>
<td>Data type</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</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>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.

### imp_user

<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>Field</td>
<td>Description</td>
<td>Data type</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>-----------</td>
</tr>
<tr>
<td>street</td>
<td>The street address of the location, for example “1234 ServiceNow way” 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 “San Diego”, “London” 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 “California”, “Connecticut” 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 “92130”, “10001” 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 “USA”, “United Kingdom” 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.
Importing data: data flow

Create a data source

Create a data source record to define what data an import set should import.

Role required: admin

1. Navigate to System Import Sets > Data Sources.
2. Click New.
3. Set the following fields.

Common data source fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique name for this data source.</td>
</tr>
<tr>
<td>Import set table label</td>
<td>Specify a label for the import set staging table to use.</td>
</tr>
</tbody>
</table>
4. Set additional fields based on the selected **Type**. Refer to the documentation for each data source type for additional field information.

5. Click **Submit**.

Define a transform map for the new data source and run an import.

**Data source fields**

Additional fields appear on the data source form depending on the value of the **Type** field.

**Field 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>Import set table name</td>
<td>ServiceNow uses the label you entered to construct a unique table name. This prevents namespace collision with an already existing table.</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Select the type of data you are importing, such as from a remote <strong>File</strong>, a <strong>JDBC</strong> database, or using <strong>LDAP</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Format</strong></td>
<td>Select one of the following formats from the list: CSV, CSV (tab), Custom (Parse by Script), Excel, JSON, XML.</td>
</tr>
<tr>
<td><strong>Zipped</strong></td>
<td>Select this check box if the import file is compressed.</td>
</tr>
<tr>
<td><strong>Xpath for each row</strong></td>
<td>Specify an 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><strong>Expand node children</strong></td>
<td>Select this check box if child elements of the XML node or JSON object should be converted into additional columns. Clear this check box 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><strong>File retrieval method</strong></td>
<td>Choose the appropriate 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>Specify the path to the file to import. You can include a system property value in this field using the format <code>$(system.property.name)</code>. When the connection is made, the variable is replaced with the value of the specified property.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>For files retrieved using HTTP or HTTPS, the property <code>glide.ds.file.http.variable_replacement</code> must be true to use system property expansion.</td>
</tr>
<tr>
<td></td>
<td>For example, you can specify the File path value <code>/countries.csv?key=$(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 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>SCP authentication method</td>
<td>Select 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>Enter the name of the server from which the file will be imported. 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 property <code>glide.ds.file.http.variable_replacement</code> must be true to use system property expansion.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the 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>User name</td>
<td>Enter the user name for authentication on the file server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for authentication on the file server.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private keyfile</td>
<td>Specify the keyfile when using legacy SCP public-private keyfiles.</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></td>
<td><strong>Note:</strong> Do not use this legacy option. While it is available for use, it is not supported.</td>
</tr>
<tr>
<td>System KeyStore</td>
<td>Select this check box to validate the certificate from the FTPS server against all saved certificates. This certificate may be any type supported by the instance. If you do not select this check box, 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>

### 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>Select a MID Server to use to connect to this data source.</td>
</tr>
<tr>
<td>Format</td>
<td>Select one of the supported database formats. Instances can connect to Microsoft SQL Server 2012 but not Microsoft SQL Server 2000.</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>Enter the name of the database instance.</td>
</tr>
<tr>
<td>Database port</td>
<td>Enter the 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>Select this check box 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 <strong>JDBC type data source</strong>.</td>
</tr>
<tr>
<td>User name</td>
<td>Enter the user name for authentication on the database server. The user name provided for the JDBC connection must be associated with an account on that database server; it cannot be a Windows Domain account.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for authentication on the database server.</td>
</tr>
<tr>
<td>Server</td>
<td>Enter the name of the server from which the data will be imported.</td>
</tr>
<tr>
<td>Query</td>
<td>Select the 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>Specify the 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>Connection timeout</td>
<td>Specify the number of seconds before MID Server connection cache pool closes and removes it from the pool. Zero means no timeout.</td>
</tr>
<tr>
<td>Table name</td>
<td>Type the name of the table from which the data is being exported.</td>
</tr>
<tr>
<td>SQL statement</td>
<td>Type a SQL statement to extract the desired data from the database.</td>
</tr>
<tr>
<td>Use last run datetime</td>
<td>This selection controls the amount of data that is retrieved from a database during an import run. If this check box is 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 this check box is 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>Select the 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. Enter a semicolon-separated list of parameters. You may need to configure the form to view this field.</td>
</tr>
</tbody>
</table>

**LDAP type data source fields**

These additional fields appear on the data source form when the **Type** field value is **LDAP**.
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. Fill in the fields, as appropriate (see table).

### Create transform map

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP target</td>
<td>Select a target from the list of your LDAP OU definitions.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter a user-friendly label for identifying the transform map.</td>
</tr>
<tr>
<td>Source table</td>
<td>Select the import table containing the raw import set data. An import table is any table that extends the Import Set Row [sys_import_set_row] table. You can select only tables within the currently selected application scope.</td>
</tr>
<tr>
<td>Active</td>
<td>Select this check box to make the transform map available for use.</td>
</tr>
<tr>
<td>Run Business Rules</td>
<td>Select this check box to run business rules, workflows, approval engines, auditing, and field normalization while the transformation inserts or updates data into the target table. Clearing this check box runs GlideRecord.setWorkflow() with a value of false.</td>
</tr>
<tr>
<td>Enforce Mandatory Fields</td>
<td>Choose whether to enforce mandatory fields on the target table.</td>
</tr>
<tr>
<td>Copy Empty Fields</td>
<td>Select this check box to clear fields with existing values when an incoming field contains an empty value. See Using NULL as a Field Value for information on how to import empty values.</td>
</tr>
<tr>
<td>Created</td>
<td>Shows the transform map creation date. This field is automatically populated.</td>
</tr>
<tr>
<td>Target table</td>
<td>Select the table where you want transformed data to be placed. You can select only tables within the currently selected application scope, the global scope, or tables that grant write access to other applications.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Order</td>
<td>Enter the order in which to apply transform maps in the event that more than one map fits the conditions. ServiceNow runs transform maps from lowest to highest Order.</td>
</tr>
<tr>
<td>Run Script</td>
<td>Select this check box to display the Script field.</td>
</tr>
<tr>
<td>Script</td>
<td>Enter the transform map script you want to use to transform field values in the source table to the target table. ServiceNow runs the transform map script in addition to any Field Maps.</td>
</tr>
<tr>
<td>Field Maps</td>
<td>Use this related list to add one or more field maps. ServiceNow runs the transform Field Maps in addition to any transform script.</td>
</tr>
<tr>
<td>Transform scripts</td>
<td>Use this related list to add one or more transform map scripts. A transform script allows you to apply extra business logic at a specified stage of the transformation.</td>
</tr>
</tbody>
</table>

The sample User import transform map looks like this.
**Table Transform Map**

- **Name:** User
- **Source table:** User [imp_user]
- **Target table:** User [sys_user]
- **Active:** Yes
- **Run business rules:** Yes
- **Enforce mandatory fields:** No
- **Order:** 100
- **Script:**

```java
/**
 * For variables go to: http://wiki.service-now.com/index.php?title=Import_sets
 */

// create a user id if necessary
if (source.user_id.nil())
7  target.user_name = source.first_name + "." + source.last_name;
```

**Related Links**
- Auto map matching fields
- Mapping Assist
- Transform

**Field Maps (7)**

<table>
<thead>
<tr>
<th>Source field</th>
<th>Target field</th>
<th>Coalesce</th>
</tr>
</thead>
<tbody>
<tr>
<td>last_name</td>
<td>last_name</td>
<td>false</td>
</tr>
<tr>
<td>department</td>
<td>department</td>
<td>false</td>
</tr>
<tr>
<td>email</td>
<td>email</td>
<td>true</td>
</tr>
<tr>
<td>phone</td>
<td>phone</td>
<td>false</td>
</tr>
<tr>
<td>first_name</td>
<td>first_name</td>
<td>false</td>
</tr>
<tr>
<td>user_id</td>
<td>user_name</td>
<td>false</td>
</tr>
<tr>
<td>location</td>
<td>location</td>
<td>false</td>
</tr>
</tbody>
</table>

**Actions on selected rows...**
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).
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:

<table>
<thead>
<tr>
<th>Mapping Options</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>
<tr>
<td>yyyy-dd-MM</td>
<td>Year-day-month</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.
5. Click **Update**.

---

© 2019 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.
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.

```java
//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.

```java
//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.

```java
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
}
```

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.
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. Fill in the fields, as appropriate (see table).
5. Click **Save**.
6. Repeat steps 3-4 for each field mapping.
7. Click **Update**.

### Creating a Field Map

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source table</td>
<td>Displays the table where the raw import set data is loaded (the source for the transformation). This field is automatically populated from the transform map. You can select only tables within the currently selected application scope.</td>
</tr>
<tr>
<td>Source field</td>
<td>Select the field on the source table to be transformed. This may be blank if the <strong>Source table</strong> only contains raw data.</td>
</tr>
<tr>
<td>Map</td>
<td>Displays the transform map that uses this field mapping. This field is automatically populated.</td>
</tr>
<tr>
<td>Date format</td>
<td>This field is available if the target field is a date or date-time field. This field specifies the date format of the source field.</td>
</tr>
</tbody>
</table>
| Choice action     | This field is available if the target field is a choice list or reference field. This field specifies what to do if the import set contains a reference or choice value other than those available. Select one of these options:  
  - **create**: Create a new choice or record in the reference table.  
  - **ignore**: Ignore the new value from the source table.  
  - **reject**: Skip the entire row (record) containing the new value and continue to the next row. |
<p>| Use source script | Select this check box to use a script instead of the <strong>Source field</strong>. |
| Source script     | Enter a script to determine the source of this field mapping instead of the <strong>Source field</strong>. The script should return the answer variable. |
| Target table      | Select the table where you want transformed data to be placed. You can select only tables within the currently selected application scope, the global scope, or tables that grant write access to other applications. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target field</td>
<td>Select the field where the values from the source field is stored.</td>
</tr>
<tr>
<td>Referenced value field 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>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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>
<tr>
<td>Coalesce empty fields</td>
<td>Select this check box to match an empty source field value to an empty target field value. For example, the User transform map coalesces on the email field. With this option selected, a source record containing an empty email address coalesces to a target record containing an empty email address.</td>
</tr>
<tr>
<td>Coalesce case sensitive</td>
<td>Select this check box to have case sensitive coalesce values result in the creation of new records. By default, values marked as Coalesce are used in a case insensitive lookup for existing records. Case insensitive records only update existing records and do not cause the creation of new records.</td>
</tr>
</tbody>
</table>

A completed field map record with coalescence enabled might look like this:
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 log.info(&quot;&lt;Message&gt;&quot;), or log.warn(&quot;&lt;Message&gt;&quot;). 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>Variable</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>action</td>
<td>String</td>
<td>Contains either the value insert or update, depending on whether the current target row will be created or updated.</td>
</tr>
</tbody>
</table>

**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

Import run history

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.
Import History Record

Schedule a data import

Scheduled imports make it is possible to specify that certain import operations should occur at some regular interval.

Role required: import_scheduler, import_admin, or admin

**Important:** Do not schedule multiple imports at the same time. Running multiple imports concurrently may negatively impact performance or cause an instance outage.

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>Enter a name for this scheduled data import.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Data source</td>
<td>Select the data source record that defines the data to import. If you select a remote data source, it is refreshed via the remote connection prior to the import operation.</td>
</tr>
<tr>
<td>Run as</td>
<td>Enter the 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>Select this check box to activate the scheduled import.</td>
</tr>
<tr>
<td>Run</td>
<td>Select the frequency at which you want to run the import.</td>
</tr>
<tr>
<td>Time</td>
<td>Enter the time you want the import to begin. Do not schedule multiple imports at the same time. Running multiple imports concurrently may negatively impact performance or cause an instance outage.</td>
</tr>
<tr>
<td>Conditional</td>
<td>Select this check box if you want to write a script to define the conditions that must evaluate to true before the import runs.</td>
</tr>
<tr>
<td>Condition</td>
<td>Write the script to be used to evaluate whether an import should run. This field is visible if you selected the Conditional check box.</td>
</tr>
<tr>
<td>Repeat interval</td>
<td>Select the period that must elapse before the import is repeated. This field is visible if Run is set to Periodically.</td>
</tr>
<tr>
<td>Starting</td>
<td>Click the calendar icon and select the date on which the import should begin. This field is visible if Run is set to Periodically.</td>
</tr>
<tr>
<td>Execute pre-import script</td>
<td>Select this check box if you want to write a script to be run before the import is performed.</td>
</tr>
<tr>
<td>Pre script</td>
<td>Write the script you want to run before the data is imported. This field is visible if you selected the Execute pre-import script check box.</td>
</tr>
<tr>
<td>Execute post-import script</td>
<td>Select this check box if you want to write a script to be run after the import is performed.</td>
</tr>
<tr>
<td>Post script</td>
<td>Write the script you want to run after the import finishes. This field is visible if you selected the Execute post-import script check box.</td>
</tr>
</tbody>
</table>

3. To stop an import that is taking too much time, navigate to **System Import Sets > Advanced > Progress**.
4. Open the Progress Worker that must be canceled.
5. Under **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.

<table>
<thead>
<tr>
<th>Object</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>cancel</td>
<td>Set this object to true to stop the import action.</td>
<td>Use the Pre script 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>
</tr>
<tr>
<td></td>
<td></td>
<td>cancel = true;</td>
</tr>
<tr>
<td>import_set</td>
<td>Get the GlideRecord object for the new import set.</td>
<td>If you want to use information from the import set, you can specify one of the properties of the import_set variable.</td>
</tr>
<tr>
<td></td>
<td>This variable allows you to query the following</td>
<td>var x = import_set.number;</td>
</tr>
<tr>
<td></td>
<td>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</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>
</tr>
<tr>
<td></td>
<td>scheduled import.</td>
<td>data_source.import_set_table_name = 'new_set_from_scheduler';</td>
</tr>
<tr>
<td></td>
<td></td>
<td>data_source.update();</td>
</tr>
</tbody>
</table>

Post CSV or Excel files directly to an import set

An administrator can post CSV or Excel files directly to 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
#!/usr/bin/perl
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,
);

# mandatory arguments: url
&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 { 

```
Java example

```java
printf "usage: %s --url=%s --uploadfile=%s\n",
    basename($0), 'https://....', 'c:/data/test.csv';
exit
}

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.

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.setRequestHeader(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();
}
```

Import Sets properties

Multiple properties control Import Set behavior.
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.import_set.preserve.leading.spaces</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Attention</strong>: The import process always removes trailing spaces from Excel data cells.</td>
</tr>
</tbody>
</table>
|                                              | • 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  
|                                              | • Default value: true  
|                                              | • Location: [Add the property](#)                                                                                                                                                                       |
| 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](#)  
<p>|                                              | • More information: <a href="#">Data source fields</a>                                                                                                                                       |</p>
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.scheduled_import.stop_on_error</td>
<td>Set this object 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.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: false</td>
</tr>
<tr>
<td></td>
<td>• Location: <a href="#">Add the property</a></td>
</tr>
<tr>
<td>glide.impex.transformer.empty_value_nil</td>
<td>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'.</td>
</tr>
<tr>
<td></td>
<td>Note: An empty string is always stored as a null value in the database, regardless of this property value.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: false</td>
</tr>
<tr>
<td></td>
<td>• Location: <a href="#">Add the property</a></td>
</tr>
<tr>
<td>com.glide.loader.max_scan_rows</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td>• Default value: 20</td>
</tr>
<tr>
<td></td>
<td>• Location: <a href="#">Add the property</a></td>
</tr>
</tbody>
</table>

**Web Service Import Sets properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.glide.ws_import_set.column_resize</td>
<td>When true, enables dynamic column resizing on import staging tables for web service import sets.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: false</td>
</tr>
<tr>
<td></td>
<td>• Location: <a href="#">Add the property</a></td>
</tr>
</tbody>
</table>
### Property

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.glide.ws_import_set.column_resize.max_row_count</td>
<td>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 <code>com.glide.ws_import_set.column_resize</code> is true. This property has a maximum value of 500,000.</td>
</tr>
<tr>
<td>· Type: Integer</td>
<td></td>
</tr>
<tr>
<td>· Default value: 100,000</td>
<td></td>
</tr>
<tr>
<td>· Location: Add the property</td>
<td></td>
</tr>
</tbody>
</table>

### CSV properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.glide.csv.loader.ignore_non_parseable_lines</td>
<td>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.</td>
</tr>
<tr>
<td>· Type: <code>true</code></td>
<td><code>false</code></td>
</tr>
<tr>
<td>· Default value: <code>false</code></td>
<td></td>
</tr>
<tr>
<td>· Location: Add the property</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.glide.csv.loader.max_errors_allowed</td>
<td>Specify 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.</td>
</tr>
<tr>
<td>· Type: integer</td>
<td></td>
</tr>
<tr>
<td>· Default value: <code>100</code></td>
<td></td>
</tr>
<tr>
<td>· Location: Add the property</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.import.csv.charset</td>
<td>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.</td>
</tr>
<tr>
<td>· Type: String</td>
<td></td>
</tr>
<tr>
<td>· Default value: <code>WINDOWS-1252</code></td>
<td></td>
</tr>
<tr>
<td>· Location: Add the property</td>
<td></td>
</tr>
</tbody>
</table>
### Excel import properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.excel.multiplier</td>
<td>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.</td>
</tr>
</tbody>
</table>
|                               |   - 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. |
|                               |   - 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 if 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](#)                                                                                                                                                                                          |
### Property

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.excel.in_memory_strings_table_size_mb</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>- Type: integer</td>
</tr>
<tr>
<td></td>
<td>- Default value: 5</td>
</tr>
<tr>
<td></td>
<td>- Location: <a href="#">Add the property</a></td>
</tr>
<tr>
<td>glide.xlsx.import.debug</td>
<td>Enables debug logging for XLSX imports.</td>
</tr>
<tr>
<td></td>
<td>- Type: true</td>
</tr>
<tr>
<td></td>
<td>- Default value: false</td>
</tr>
<tr>
<td></td>
<td>- Location: <a href="#">Add the property</a></td>
</tr>
<tr>
<td>glide.import.excel.enhanced_number_conversions</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>- Type: true</td>
</tr>
<tr>
<td></td>
<td>- Default value: true</td>
</tr>
<tr>
<td></td>
<td>- Location: <a href="#">Add the property</a></td>
</tr>
</tbody>
</table>

### JDBC Connection Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.jdbcprobeloader.retry</td>
<td>The number of times a JDBC probe loader attempts to process data returning from a JDBC data source. Sleeps on the value defined in &quot;glide.jdbcprobeloader.retry_millis&quot; between retries.</td>
</tr>
<tr>
<td></td>
<td>- Type: integer</td>
</tr>
<tr>
<td></td>
<td>- Default value: 60</td>
</tr>
<tr>
<td></td>
<td>- Location: <a href="#">Add the property</a></td>
</tr>
<tr>
<td>glide.jdbcprobeloader.retry_millis</td>
<td>How many milliseconds a JDBC probe loader waits in between retry attempts to process data from a JDBC data source.</td>
</tr>
<tr>
<td></td>
<td>- Type: integer</td>
</tr>
<tr>
<td></td>
<td>- Default value: 5000</td>
</tr>
<tr>
<td></td>
<td>- Location: <a href="#">Add the property</a></td>
</tr>
</tbody>
</table>
## Logging and debug properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 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 to the System Property (sys_properties) table |
| 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 to the System Property (sys_properties) table |
| 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 to the System Property (sys_properties) table |

## Web service import sets

Web Service Import Sets complement Direct Web Services and Scripted Web Services in providing a web service interface to Import Set tables.
This type of web service will transform the incoming data synchronously based on the associated transform maps by default. 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

Web service import set WSDL are accessed by specifying the import set table name + ".do?WSDL" on the URL. For example:

http://<instance name>.service-now.com/imp_notification.do?WSDL (The System Web Service plugin must be enabled first)

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 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

```javascript
// 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:Header/>
<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.

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.

### Import Set Mode

<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 Loaded</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>
<tr>
<td>Mode</td>
<td>State</td>
<td>Function</td>
</tr>
<tr>
<td>--------------</td>
<td>--------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Synchronous</td>
<td>Loaded</td>
<td>When new data is inserted into this associated import set, a new import set of mode Synchronous and state Loading will be created. Changing the state to Loaded is a way to indicate that a new Synchronous import set should be created for the next import set row insert (and transformed immediately)</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
  <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>
```

**Field 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>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>table</td>
<td>The table name of the table that was affected. In the case of an Asynchronous call, the table name would be the import set table eg. imp_notification for the Notifications 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 Incident table is the Number 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>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 'ignored'. 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 error. 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.
**Note:** Activating this plugin adds a new operation to the SOAP WSDL. After this plugin is activated, consume a new WSDL to update your web services client.

**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"?>
<wsdl:definitions
  targetNamespace="http://www.service-now.com"
  xmlns:tns="http://www.service-now.com/imp_notification"
  xmlns:sncns="http://www.service-now.com"
  xmlns:mime="http://schemas.xmlsoap.org/wsdl/mime/"
  xmlns:http="http://schemas.xmlsoap.org/wsdl/http/"
  xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
>
  <wsdl:types>
    <xsd:schema
      xmlns:xsd="http://www.w3.org/2001/XMLSchema"
      elementFormDefault="unqualified"
      targetNamespace="http://www.service-now.com/imp_notification">
      <xsd:element namespace="insert">
        <xsd:complexType>
          <xsd:sequence>
            <xsd:element maxOccurs="1" minOccurs="0"
              name="corrective_message" type="xsd:string"/>
            <xsd:element maxOccurs="1" minOccurs="0"
              name="duration" type="xsd:string"/>
            <xsd:element maxOccurs="1" minOccurs="0"
              name="expires_on" type="xsd:string"/>
            <xsd:element maxOccurs="1" minOccurs="0"
              name="message" type="xsd:string"/>
            <xsd:element maxOccurs="1" minOccurs="0"
              name="severity" type="xsd:string"/>
            <xsd:element maxOccurs="1" minOccurs="0"
              name="source" type="xsd:string"/>
            <xsd:element maxOccurs="1" minOccurs="0"
              name="timestamp" type="xsd:string"/>
            <xsd:element maxOccurs="1" minOccurs="0"
              name="type" type="xsd:string"/>
            <xsd:element maxOccurs="1" minOccurs="1"
              name="uuid" type="xsd:string"/>
          </xsd:sequence>
        </xsd:complexType>
      </xsd:element>
      <xsd:element namespace="insertResponse">
        <xsd:complexType>
          <xsd:sequence>
            <xsd:element maxOccurs="1" minOccurs="1"
              name="sys_id" type="xsd:string"/>
            <xsd:element maxOccurs="1" minOccurs="1"
              name="table" type="xsd:string"/>
            <xsd:element maxOccurs="1" minOccurs="1"
              name="display_name" type="xsd:string"/>
            <xsd:element maxOccurs="1" minOccurs="1"
              name="display_value" type="xsd:string"/>
            <xsd:element maxOccurs="1" minOccurs="0"
              name="status" type="xsd:string"/>
            <xsd:element maxOccurs="1" minOccurs="0"
              name="status_message" type="xsd:string"/>
            <xsd:element maxOccurs="1" minOccurs="0"
              name="error_message" type="xsd:string"/>
          </xsd:sequence>
        </xsd:complexType>
      </xsd:element>
    </xsd:schema>
  </wsdl:types>
  <wsdl:message name="insertSoapOut">
    <wsdl:part
      name="imp_notification" element="tns:insertResponse"/>
  </wsdl:message>
  <wsdl:message name="insertSoapIn">
    <wsdl:part
      name="imp_notification" element="tns:insert"/>
  </wsdl:message>
  <wsdl:portType name="ServiceNowSoap"/>
  <wsdl:binding
    type="sncns:ServiceNowSoap">
    <soap:binding
      style="document"
      transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="insert">
      <soap:operation
        soapAction="http://www.service-now.com/imp_notification/insert">
        <wsdl:input
          message="sncns:insertSoapIn"/>
        <wsdl:output
          message="sncns:insertSoapOut"/>
      </soap:operation>
    </wsdl:binding>
  </wsdl:portType>
</wsdl:definitions>
```

© 2019 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.
Sample SOAP Envelope

```xml
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:xsd="http://www.w3.org/2001/XMLSchema"
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <SOAP-ENV:Body>
    <insert xmlns="http://www.service-now.com">
      <message xsi:type="xsd:string">Host 198.10.10.210 is down</message>
      <uuid xsi:type="xsd:string">HGAF76251HGF1</uuid>
    </insert>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Sample SOAP Response

```xml
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  <SOAP-ENV:Body>
    <insertResponse>
      <sys_id>b54aafbfcoa800f0058db5da5b88d</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 => {} );
sub SOAP::Transport::HTTP::Client::get_basic_credentials { return 'itil' => 'itil'; };

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_fault {my($result)=@_;if($result->{fault}){print"faultcode=".
$result->{fault}->{\'faultcode\'}."\n";print"faultstring=".$result->{fault->
>(\'faultstring\')}."\n";print"detail=".$result->{fault->\{\'detail\'}."\n";}}}

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=cd45649c0a0a0b2b00e6f27649d6bd2c

The following image shows the resultant row created for the import set table Notification (imp_notification).

<table>
<thead>
<tr>
<th>Created</th>
<th>Set</th>
<th>State</th>
<th>Target record</th>
<th>Message</th>
<th>Severity</th>
<th>Source</th>
<th>UUID</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009-01-12 15:55:23</td>
<td>ISET10002</td>
<td>Inserted</td>
<td>Incident INC10011</td>
<td>problem detected for database DB12DG</td>
<td></td>
<td></td>
<td>GIAF76251HGF2</td>
<td></td>
</tr>
</tbody>
</table>

**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 uses 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 use 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 Import</td>
</tr>
<tr>
<td>List v3</td>
<td>Open the list title menu and select Import</td>
</tr>
</tbody>
</table>
3. From Insert or update, select the import type.
4. 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.

**Easy import template validation**

Each import template must pass two sets of validation.

**Template 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>
<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

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</td>
</tr>
<tr>
<td></td>
<td>applies only to fields in which the list of possible choices is relatively</td>
</tr>
<tr>
<td></td>
<td>small and mostly static. It does not apply to fields such as ‘Assigned To’ in</td>
</tr>
<tr>
<td></td>
<td>which the list of possible choices is dynamic and large. Validation takes</td>
</tr>
<tr>
<td></td>
<td>place when the data is inserted into the database, but not in Excel.</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.

| True | False | Cell contains a true or false value. |

Easy import properties
Several properties control the behavior of easy import.
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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  
- Default value: table_name, order_index, collection, user_image, video, timer, translated_field, conditions, field_name, sys_class_name, journal, journal_input, due_date, user_input, image, workflow, template_value, domain_id, documentation_field, user_roles, glide_list  
- Location: Add the property |

**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.

**Symtoms:** 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**

**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 ServiceNow Technical 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:

```xml
<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:

```xml
<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:

```xml
<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)
- Group Roles (sys_group_has_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:
   - Format: XML
   - Import set table label: <import_set_table_label>
   - Xpath root node: <source_table_name>
   - Expand node children: true.
   - File retrieval method: HTTPS
   - File path: <source_table_name>.do?XML
   - Server: <instance name>.service-now.com
   - Username: A user account on the remote instance. The username used cannot be an email address.
   - Password: The password for the same remote account.
4. Click Submit.
5. Click Test Load 20 Records to create the import set table and to ensure your data source is functional.

Note:
The 20 loaded records cannot 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.
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

   ![Data Source Form]

**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

The system clone application allows users with the clone_admin or admin role to clone data from one instance to another.

This functionality is primarily used to clone a production instance over an existing sub-production instance before developing or testing changes. All clones are performed using the most recent nightly backup.

![Clone process diagram]

**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.
   
   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.
   Certain 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 ServiceNow Technical 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 platform uses data from the most recent nightly backup of the source instance when cloning. Backups used for cloning are at most 36 hours old. System Clone begins the initial preparation process, including selecting the latest backup to use, only at the date and time processing is scheduled to commence.

If a clone from backup fails for any reason, the system instead uses 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 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

Production instances cannot be used as the target instance for a clone after the instance is live. Production clones are created during non-core business hours. Tables are backed up sequentially rather than simultaneously. Modifying data on the source instance during a clone can cause a data mismatch between records or duplicate record entries. This issue is minimized by running a clone after normal business hours.

When scheduling a clone for a production instance, the system automatically follows this process:

- Determines the instance region.
- Determines the non-core business hours for the region.
- Restricts the possible cloning time that can be specified on the Clone Request form to the non-core hours.

<table>
<thead>
<tr>
<th>Region</th>
<th>Non-core business hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Americas East Coast</td>
<td>23:00 to 04:00 Eastern time (UTC −5) and all day Saturdays and Sundays</td>
</tr>
<tr>
<td>Americas West Coast</td>
<td>20:00 to 01:00 Pacific time (UTC −8) and all day Saturdays and Sundays</td>
</tr>
<tr>
<td>Australia</td>
<td>23:00 to 04:00 Australian Eastern time (UTC +10) and all day Saturdays and Sundays</td>
</tr>
<tr>
<td>Europe Amsterdam</td>
<td>00:00 to 05:00 Central European time (UTC +1) and all day Saturdays and Sundays</td>
</tr>
<tr>
<td>Europe London</td>
<td>23:00 to 04:00 British time (UTC) and all day Saturdays and Sundays</td>
</tr>
<tr>
<td>Asia Hong Kong</td>
<td>23:00 to 04:00 Hong Kong time (UTC +8) and all day Saturdays and Sundays</td>
</tr>
</tbody>
</table>
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 platform uses data from the most recent nightly backup of the source instance when cloning. Backups used for cloning are at most 36 hours old. System Clone begins the initial preparation process, including selecting the latest backup to use, only at the date and time processing is scheduled to commence.

If a clone from backup fails for any reason, the system instead uses 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 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.

1. Login to the instance you want to clone.
   This instance becomes the source instance of the clone request.
2. Create a clone target record for each target instance you want to receive clone data.
3. Verify the list of tables excluded from cloning and add or remove tables to exclude from the target instance.
4. Verify the list of tables and system properties that will be saved on the target instance by data preservers and create or modify data preservers as needed.

   The legacy clone engine does not support data preservers for these records.
   - Tables that extend Task
   - Relationships
   - Hierarchies
   - Dot-walked queries

   If you are preserving any data not supported by the legacy clone engine, verify there is a recent backup of the target instance available. Should the clone-from-backup-process fail for any reason, you can restore the target instance from the backup.
5. Preserve any unpublished applications on the target instance.
7. Select the Target instance to receive the cloned data.
   You must create a separate clone request for each target instance you want to receive clone data.
8. Complete the Options form section.
### Clone options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exclude tables specified in Exclusion List</td>
<td>Prevent 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></td>
<td><strong>Note:</strong> This option is not supported by the legacy clone engine.</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>
<tr>
<td>Exclude large attachment data</td>
<td>Prevents the cloning of large attachments such as video files, image files, and other typically large binary file types. Excludes 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.</td>
</tr>
<tr>
<td></td>
<td>* The attachment table_name value does not indicate it is a small file. Small attachments have table name values that start with ZZ_.</td>
</tr>
<tr>
<td></td>
<td>* The attachment data type value indicates it is a large file such as application or video.</td>
</tr>
<tr>
<td></td>
<td>* 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.</td>
</tr>
<tr>
<td></td>
<td>This option is selected by default.</td>
</tr>
<tr>
<td>Amount of data copied from the Task table</td>
<td>Select the amount of data to clone from the source instance Task table. By default, the target instance receives the last 90 days of Task table records from the source instance.</td>
</tr>
<tr>
<td>Preserve theme</td>
<td>Enables data preservers for the target instance theme and CSS elements. This option is selected by default.</td>
</tr>
</tbody>
</table>

9. Select the **Clone Scheduled Start Time**.

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 need to occur sequentially.
The system verifies the scheduled start time and either accepts the date-time value 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 **Email upon completion**, enter an address to receive alerts after the clone finishes, is canceled, or has an error.

11. Click **Submit**. The system displays an authentication window.

12. Enter the **Username** and **Password** for an administrator account on the target instance.

13. 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.

If necessary, you can [cancel your clone request](#). For clones that have completed, you can [view the clone history](#).

**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. 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.

**Clone target invalid**

4. Enter the basic authentication credentials for a user account with the admin role on the target instance.
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.

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

Data 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 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)

### 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>
<tr>
<td>Name</td>
<td>Table</td>
<td>Conditions</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Core Instance Properties</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.

<table>
<thead>
<tr>
<th>Digest Properties</th>
<th>Digest Properties (digest_properties)</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Providers</td>
<td>Identity Providers (sso_properties)</td>
<td>None</td>
</tr>
<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, a good practice is to avoid changing them. 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 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).
- 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. If, however, a table you want to preserve is on the target but not on the source, use the following procedure on the target and then import the clone_data_preserver file to the source.

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.
4. Select the Table to be preserved.
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.

**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)
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>Application version state</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>The application is only available on the clone target instance.</td>
<td>(Recommended) Link each application to a source control repository.</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.

<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>Application installation state</td>
<td>Action to take on clone target</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------</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>
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 of time a clone remains active varies depending on 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 system stops any current clone activities and sets the State to Canceled.

If you want to restart a canceled clone, click Restart Clone, otherwise you can create a new clone request.

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.
## Clone states

<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>
</tbody>
</table>

2. Select a System Clone record to view its history.

### 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 is 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**.

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>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 System ID and Claimed by 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 contained in the target instance database prior to the clone. This original data is preserved for 24 hours following a clone to allow 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.

With data constantly being added to the system, and activity being logged into system tables in the database, these tables grow in size and require management. As data sets increase in size, the amount of I/O traffic associated with actions such as cleaning, deleting, and archiving can negatively effect the performance of an instance. Additionally, working with all rows in a data set, rather than a smaller working set, can create unnecessary risk.

The Database Rotation plugin preserves instance performance and averts risk associated with querying growing data sets utilizing two techniques. Both techniques are based on the concept of managing large quantities of data by separating whole sets into individual tables based on user-specified time parameters. 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 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 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) or Rotation (deletion) 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 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 Definition > Plugins**.
2. Find and click the plugin name.
3. On the System Plugin form, review the plugin details and then click the **Activate/Upgrade** related link.
If the plugin depends on other plugins, these plugins are listed along with their activation status.

If the plugin has optional features that depend on other plugins, those plugins are listed under the **Some files will not be loaded because these plugins are inactive**. The optional features are not installed until the listed plugins are installed (before or after the installation of the current plugin).

4. **Optional**: If available, 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 practice when you first activate the plugin on a development or test instance.

You can also load demo data after the plugin is activated by clicking the **Load Demo Data Only** related link on the System Plugin form.

5. **Click Activate**.

Do not activate the **Database Rotations Default Tables** plugin. Instead, specify the tables manually, after consulting a ServiceNow representative.

**Domain separation and Data Management**

This is an overview of domain separation and Data Management. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can then control several aspects of this separation, including which users can see and access data.

**Overview**

Domain separation is not supported in this application. For more information, see [Application support for domain separation](#).

**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
ServiceNow 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>Integration</td>
<td>Type</td>
<td>Integration Point</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Verizon eBonding</td>
<td>Web services</td>
<td>Incident</td>
</tr>
</tbody>
</table>

**Set up Google Maps API**

Map pages enable you to graphically display data on a Google map page based on location data.

Role required: admin

Maps can be generated using basic JavaScript, but are flexible enough to display even the most complicated of queries. The maps you generate use standard Google Maps API mapping features, including various link types to records in your instance. This feature requires the Google Maps plugin.

![Google Maps Image](image_url)

**Map page**

1. If necessary, obtain a Google Maps for Work license key to cover development use of the Google Maps API. See the [Getting Started Guide](#) on the Google web site for details on obtaining a key, using the API, and relevant terms of service.

2. When you receive your key, enter it in the System Properties > Google Maps property form, and configure your maps using the property definitions from the table.

3. After you complete the configuration, create map pages or use the default pages included with the plugin. Map pages define what data is displayed on the map and the appearance of the links. For a tutorial on how to display all markers that link to your records, see the [Display Map Markers on Google Maps](#) blog post on theNow Community.
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| google.maps.auto_close      | If true, automatically closes a map information window before opening a new one.  
  • Type: true/false  
  • Default value: true  
  • Location: System Properties > Google Maps                                                                                                                                                                                                                                    |
| google.maps.client          | Client ID for Google Maps API for Work.  
  • Type: string  
  • Default value: gme-servicenow  
  • Location: System Properties > Google Maps                                                                                                                                                                                                                                    |
| google.maps.private.key     | Private key for Google Maps API for Work. This key activates the geolocation feature, which locates users in the system precisely, using data from their mobile devices.  
  • Type: string  
  • Default value: empty  
  • Location: System Properties > Google Maps                                                                                                                                                                                                                                    |
| google.maps.version         | Version number of the current installation of Google Maps API.  
  • Type: string  
  • Default value: current version number  
  • Location: System Properties > Google Maps                                                                                                                                                                                                                                    |
| google.maps.key             | The Google Maps API key that is tied to the URL of the server. This key authorizes development use of Google Maps API.  
  • Type: string  
  • Default value: empty  
  • Location: System Properties > Google Maps                                                                                                                                                                                                                                    |
| google.maps.latitude        | Starting latitude of the map. This value determines the starting position displayed in Google Maps.  
  • Type: string  
  • Default value: 36.008522  
  • Location: System Properties > Google Maps                                                                                                                                                                                                                                    |
## ServiceNow London Now Platform Administration

### Property | Description
--- | ---
`google.maps.longitude` | Starting longitude of the map. This value determines the starting position displayed in Google Maps pages.  
- Type: string  
- Default value: -95.221764  
- Location: System Properties > Google Maps

`google.maps.max_items` | Maximum number of items to display on the map.  
- Type: integer  
- Default value: 500  
- Location: System Properties > Google Maps

`google.maps.table` | Table used by the map. The table needs the following fields: name, longitude, latitude.  
- 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: string  
- Default value: 4  
- Location: System Properties > Google Maps

### Activate Google custom search integration

The Google Custom Search Integration plugin is available by request.  
Role required: none  
Request the plugin through the HI Service Portal.  
1. In the HI Service Portal, click Service Requests > Activate Plugin.  
2. Fill out the form.

<table>
<thead>
<tr>
<th>Target Instance</th>
<th>Instance on which to activate the plugin.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plugin Name</td>
<td>Name of the plugin to activate.</td>
</tr>
</tbody>
</table>
Specify the date and time you would like this plugin to be enabled

<table>
<thead>
<tr>
<th>Date and time must be at least 2 business days from the current time.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong> Plugins are activated in two batches each business day in the Pacific time zone, once in the morning and once in the evening. If the plugin must be activated at a specific time, enter the request in the Reason/Comments.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reason/Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide any information that would be helpful for the ServiceNow personnel activating the plugin. For example, if you need the plugin activated at a specific time instead of during one of the default activation windows.</td>
</tr>
</tbody>
</table>

3. 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.

The Integration - Microsoft SCCM 2016 (com.snc.integration.sccm2016) plugin is compatible with SCCM version 1702 and 1802.

**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 Definition > Plugins**.
2. Find and click the plugin name.
3. On the System Plugin form, review the plugin details and then click the **Activate/Upgrade** related link.
   
   If the plugin depends on other plugins, these plugins are listed along with their activation status.
   
   If the plugin has optional features that depend on other plugins, those plugins are listed under **Some files will not be loaded because these plugins are inactive**. The optional features are not installed until the listed plugins are installed (before or after the installation of the current plugin).
4. Optional: If available, 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 practice when you first activate the plugin on a development or test instance.
   
   You can also load demo data after the plugin is activated by clicking the **Load Demo Data Only** related link on the System Plugin form.
5. Click **Activate**.

### 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.

<table>
<thead>
<tr>
<th>SCCM table</th>
<th>Staging table</th>
<th>CMDB table</th>
</tr>
</thead>
<tbody>
<tr>
<td>v_GS_Computer_System</td>
<td>SCCM &lt;version&gt; Computer Identity</td>
<td>Computer (cmdb_ci_computer)</td>
</tr>
<tr>
<td>v_GS_Workstation_Status</td>
<td>imp_sccm&lt;version&gt;_computer_id</td>
<td></td>
</tr>
<tr>
<td>v_GS_System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>v_GS_PC_Bios</td>
<td>SCCM &lt;version&gt;</td>
<td></td>
</tr>
<tr>
<td>v_GS_Operating_System</td>
<td>imp_sccm&lt;version&gt;_os</td>
<td>Computer (cmdb_ci_computer)</td>
</tr>
<tr>
<td>v_GS_Computer_System_Product</td>
<td>imp_sccm&lt;version&gt;_product</td>
<td></td>
</tr>
<tr>
<td>v_GS_System_Enclosure</td>
<td>SCCM &lt;version&gt;</td>
<td></td>
</tr>
<tr>
<td>v_GS_Baseboard</td>
<td>imp_sccm&lt;version&gt;_baseboard</td>
<td></td>
</tr>
<tr>
<td>v_GS_Disk</td>
<td>SCCM &lt;version&gt; Disk</td>
<td>Disk (cmdb_ci_disk)</td>
</tr>
<tr>
<td>v_GS_Disk</td>
<td>imp_sccm&lt;version&gt;_disk</td>
<td></td>
</tr>
<tr>
<td>v_GS_Network_Adapter_Configuration</td>
<td>SCCM &lt;version&gt; Network</td>
<td>Network Adapter (cmdb_ci_network_adapter)</td>
</tr>
<tr>
<td>v_GS_Network_Adapter_Configuration</td>
<td>imp_sccm&lt;version&gt;_network</td>
<td></td>
</tr>
<tr>
<td>v_GS_Operating_System</td>
<td>SCCM &lt;version&gt; Operating System</td>
<td>Computer (cmdb_ci_computer)</td>
</tr>
<tr>
<td>v_GS_Operating_System</td>
<td>imp_sccm&lt;version&gt;_os</td>
<td></td>
</tr>
<tr>
<td>v_GS_Processor</td>
<td>SCCM &lt;version&gt; Processor</td>
<td>Computer (cmdb_ci_computer)</td>
</tr>
<tr>
<td>v_GS_Processor</td>
<td>imp_sccm&lt;version&gt;_processor</td>
<td></td>
</tr>
<tr>
<td>v_GS_Add_Remove_Programs</td>
<td>SCCM &lt;version&gt; Software</td>
<td>Software (cmdb_ci_spkg)</td>
</tr>
<tr>
<td>v_GS_Add_Remove_Programs_64</td>
<td>imp_sccm&lt;version&gt;_software</td>
<td></td>
</tr>
<tr>
<td>v_GS_Add_Remove_Programs_64</td>
<td>imp_sccm&lt;version&gt;_software</td>
<td></td>
</tr>
<tr>
<td>SCCM_Ext.Add_Remove_Programs</td>
<td>SCCM &lt;version&gt; Removed Software</td>
<td>Software (cmdb_ci_spkg)</td>
</tr>
<tr>
<td>SCCM_Ext.Add_Remove_Programs_64</td>
<td>imp_sccm&lt;version&gt;_removed_sw</td>
<td></td>
</tr>
<tr>
<td>SCCM_Ext.Add_Remove_Programs_64</td>
<td>imp_sccm&lt;version&gt;_removed_sw</td>
<td></td>
</tr>
<tr>
<td>SCCM_Ext.Add_Remove_Programs_64</td>
<td>imp_sccm&lt;version&gt;_removed_sw</td>
<td></td>
</tr>
</tbody>
</table>

*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.
- 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. 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.

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 credentials to query the SQL Server that contains the SCCM database.

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.
### Scheduled Data Import

**SCCM System 2010 Import**

<table>
<thead>
<tr>
<th>Name</th>
<th>SCCM System 2010 Import</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run</td>
<td>Daily</td>
</tr>
<tr>
<td>Time</td>
<td>Hours: 02, 30, 00</td>
</tr>
<tr>
<td>Active</td>
<td></td>
</tr>
<tr>
<td>Execute pre-import script</td>
<td>No</td>
</tr>
<tr>
<td>Execute post-import script</td>
<td>No</td>
</tr>
</tbody>
</table>

### Run the following imports when complete

<table>
<thead>
<tr>
<th>Name</th>
<th>Active</th>
<th>Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCCM 2016 Operating System</td>
<td>true</td>
<td>10</td>
</tr>
<tr>
<td>SCCM 2016 Processor</td>
<td>true</td>
<td>20</td>
</tr>
<tr>
<td>SCCM 2016 Disk</td>
<td>true</td>
<td>30</td>
</tr>
<tr>
<td>SCCM 2016 Network</td>
<td>true</td>
<td>40</td>
</tr>
<tr>
<td>SCCM 2016 Software</td>
<td>true</td>
<td>50</td>
</tr>
<tr>
<td>SCCM 2016 Export Software</td>
<td>true</td>
<td>60</td>
</tr>
</tbody>
</table>
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.

To activate the AI scheduled imports:
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 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 is 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 support 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

Note: 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.
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.
### Edit Web Service

<table>
<thead>
<tr>
<th>Label:</th>
<th>Altitris vComputer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
<td>imp_altitris_vcomputer</td>
</tr>
</tbody>
</table>

#### Related Links

- Import Sets
- Input Rows
- Transform History

---

Changes made to this list will be saved when the Edit Web Service form above is saved

#### Web Service Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Name</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreatedDate</td>
<td>u_createddate</td>
<td>Default (40)</td>
</tr>
<tr>
<td>Domain</td>
<td>u_domain</td>
<td>Default (40)</td>
</tr>
<tr>
<td>Guid</td>
<td>u_guid</td>
<td>Default (40)</td>
</tr>
</tbody>
</table>

---

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
   - 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.

Here is a screen shot of the result of calling the above mentioned URL:

![Screen Shot](image-url)
Integrating ServiceNow with your Intranet

There are several ways you can add a ServiceNow login link to your intranet.

You can add a login link by:

- Enabling the PortletLogin Script include to be Client Callable.
- Creating a simple HTML link to your instance that takes your users directly to the ServiceNow login page.
- Adding an iframe link to the ServiceNow login portlet in one of your HTML pages to permit direct login.

Note: The ServiceNow login portlet is the only content supported within an iframe HTML element. To deliver ServiceNow content from a web page, see Service Portal instead.

Creating a Simple Link

Edit a web page on your intranet and add a direct link to your ServiceNow instance.

For example:

```html
<a href="https://yourinstance.service-now.com">Help Desk</a>
```

Enabling the PortletLogin Script include to be Client Callable

The login portlet (https://yourinstance.service-now.com/portal/login.html) uses the PortletLogin Script Include.

Since this script is not client callable by default, you must enable the client callable option.

1. Navigate to System UI > Script Includes.
2. Open the script PortletLogin.
3. Check the Client Callable check box.
4. Click Update.

Add the Login Portlet

Adding the login portlet to an iframe HTML element creates an unbranded user and password prompt on any HTML page.

The user enters their user id and password and either presses the ENTER key or clicks the Login button. Once validated, the browser transfers to the logged-in ServiceNow session.

The portlet’s size is 240 pixels wide and 125 pixels high. The portlet looks like:

```html
User: 
Password: 
Login
```

Portal Login

Note: The ServiceNow login portlet is the only content supported within an iframe HTML element. To deliver ServiceNow content from a web page, see Service Portal instead.

To enable the login portlet:

1. Set the high security properties glide.security.use_csrf_token and glide.set_x_frame_options to false.
2. Add the following HTML code to your portal:

```html
<iframe border="0" frameborder="0" width="240" height="125" src="https://yourinstance.service-now.com/portal/login.htm" /><
```

If you do not want to change your instance's High Security settings, create a simple link instead.

**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 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)

**Related Links**

- Test Load 20 Records
- Load All Records

![Transforms](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.

```sql
select * from <table_name>
```

For example, using the following XML payload

```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=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
<?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

```xml
<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>
</table>
| jdbc_driver | Required. Java class name for the JDBC driver to use, the currently supported drivers are:  
  · Oracle: `oracle.jdbc.OracleDriver`
  · Microsoft SQL Server: `com.microsoft.sqlserver.jdbc.SQLServerDriver`
  · MySQL: `com.mysql.jdbc.Driver`                                           |

Example

```java
com.microsoft.sqlserver.jdbc.SQLServerDriver
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| connection_string | Required. JDBC connection string(URL) for defining the connection, usually contains information about the database server and name, the user ID and password for connecting to the database. The syntax is vendor specific, refer to the following links for reference:  
  · Oracle: `[jdbc:oracle:thin:<username>/<password>@<database>]`
  · Microsoft SQL Server: `[jdbc:sqlserver://localhost;user=MyUserName;password=*****;]`
  · MySQL: `[jdbc:mysql://localhost/database?user=username%26password=passwd]`

Example

```java
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>
</table>
| work      | Required if not using the `table_name` parameter short cut.  
  Parent element of an XML fragment describing the SQL command to execute. |

Example

```
...  
<pараметer name="work">  
<select table = "System.DATA" where = "InstanceKey=692"  
><MachineID /></><SMSID0 /></select></parameter>
```
<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

Example

```sql
... select * from any_table where id = 123 ...
...```
- Database server
- Database name
- User name
- User password

- The table name

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=17a31f380a0bade0048ca875c8891d0</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=17a31f380a0bade0048ca875c8891d0</URL><Severity quoted = "false">
```
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 this Wiki 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.

![Search Bar Image]

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
<?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?nav_to.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.


   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 then control several aspects of this separation, including which users can see and access data.

Overview

Support: Data only

Domain separation in this application is supported at the Data only level, meaning it supports the data security model of separating visibility of data from one domain to another. To learn more, see Application support for domain separation.

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.

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

1. Navigate to the System Properties (sys_properties) table.
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.

Request activation of the **Explicit roles** (`com.glide.explicit_roles`) plugin. The Explicit Roles plugin creates two roles to differentiate between internal and external users.

**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.

<table>
<thead>
<tr>
<th>Company fields</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>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</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:**

- **Latitude**
  - The latitude 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. 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 `Old Latitude`. The system attempts to convert all latitude values from previous versions to the floating point notation, where possible.

- **Longitude**
  - 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.

**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 overview*.

## 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 or itil

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>Last name</td>
<td>Enter the user’s last name.</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>
</tbody>
</table>

© 2019 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>Input Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Integration User</td>
<td>Select this check box to designate this user as an \textit{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 \textit{deactivate} the validation script first.</td>
</tr>
<tr>
<td></td>
<td>1. Navigate to System Definition &gt; Validation Scripts.</td>
</tr>
<tr>
<td></td>
<td>2. Select the email record.</td>
</tr>
<tr>
<td></td>
<td>3. Clear the \texttt{Active} check box and save the change.</td>
</tr>
<tr>
<td></td>
<td>4. Complete the user profile, including the email address, and update or submit the record.</td>
</tr>
<tr>
<td></td>
<td>5. Reactivate the email validation script.</td>
</tr>
<tr>
<td>Notification</td>
<td>Select the type of notification to send to this user. The default is Email. If you select None, the user can still receive notifications if they subscribe to the notification or are specified as a recipient in the Email Notifications form.</td>
</tr>
<tr>
<td></td>
<td>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 None.</td>
</tr>
<tr>
<td>Calendar integration</td>
<td>Select Outlook to have this user receive meeting notifications via email directly to the calendar. Otherwise, select None.</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 Geolocation tracked 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: \texttt{Customize the form} to add the Schedule field and assign a \texttt{schedule} to the user.

4. Optional: \texttt{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 \texttt{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 (<strong>TRUE</strong>), or not (<strong>FALSE</strong>).</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 <strong>User</strong> is blank, the record is for a system-wide default.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</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.

**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 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. The impersonation option is not visible in the mobile view of the platform.

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.
- Impersonating a user is not supported for mobile phones. For most mobile phones, however, you can impersonate a user by switching to standard view, performing the impersonation, and switching back to mobile view. Some mobile devices may have problems rendering the Impersonation dialog.

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 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.

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>glide.sys.log_impersonation</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>glide.sys.log_impersonation.non_interactive</td>
<td>Enables (true) or disables (false) impersonation logging for non-interactive sessions.</td>
</tr>
<tr>
<td>glide.sys.log_impersonation.non_interactive.exclusion</td>
<td>Excludes impersonation logging of non-interactive sessions for specified users. Enter user names as a comma-separated list. Default users (system, soap.guest, and guest) 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. **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.

Making a user inactive does not lock out the user. The Lock Out Inactive Users business rule, which is active by default in all instances, sets the **Locked Out** flag to `true` on the User record when the Active flag is set to `false`. If you do not have this business rule active, inactive users are not automatically locked out and can still log in the instance.

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 or itil

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>
</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 Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 <strong>Assigned to</strong> lookup icon, only the members in the parent group are available. The members of the child group are not available.</td>
</tr>
</tbody>
</table>
| Active         | 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:  
  - lists of groups  
  - the reference lookup list for reference fields  
  - the auto-complete list of groups displayed when you type into a reference field |
| Exclude manager| Check box that controls whether the group manager receives email notifications.                                                                                                                               |
| 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 or itil

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 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:

```java
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.

### Skills Management

The Skills Management feature enables an administrator to assign configured competencies, called skills, to groups or individual users. These skills can then be used to determine who can be assigned to particular tasks.

Skills can contain other skills. Any access granted to a parent skill is granted to any skill that it contains. Once a skill is assigned to a group, all members of the group automatically inherit that
skill and any others contained within it. The skills mechanism is similar to the ServiceNow platform role management.

Create a skill

You can create skills to specify the competencies of your users.

Role required: skill_admin or admin

1. Navigate to Skills > Skills.
2. Click New.
3. Enter a unique, descriptive Name.
4. Enter a Description of the skill.
5. Right-click the form header and click Save.

The Contains Skills, Users, and Models related lists appear.

6. Optional: Use the Contains Skills related list to add subskills.
7. Optional: Use the Models related list to add any models that are associated with the skill.

The Users related list contains users (based on their User record or the groups they belong to) who have the skill and subskills named in this record. You can also add users to specify they have the skill.

Assign a user skill

You can assign skills individually to users. If you assign a skill that contains other skills to a user, the user automatically inherits the contained skills.

Role required: skill_admin or admin

1. Navigate to Skills > Users.
2. Select a user from the list.
3. In the User record, select the Skills related list.
4. Click Edit and select one or more existing skills from the slushbucket.
5. Click Save.

Assign a group skill

You can assign skills to groups, and the members of the group inherit all the assigned skills. If you assign a skill that contains other skills to a group, the group and all its members automatically inherit the contained skills.

Role required: skill_admin or admin

1. Navigate to Skills > Groups.
2. Select a group from the list.
3. In the Group record, select the Skills related list.
4. Click Edit and select one or more existing skills from the slushbucket.
5. Click Save.

The skill is added to the group and all the group members who are granted this skill are listed at the top of the form.
Filter potential assignees based on skills

In the base system, field service management tasks and project tasks use skills to filter assignments. If a skill is identified in the **Skill** field, only groups or users with the appropriate skill can be assigned to the task.

The Skills Management feature contains a script include that builds a qualifier based on the assignment group and required skills for the task. For example, the **Assigned To** field on the Project Task record uses the following reference qualifier (using a dictionary override):

```
javascript:var util = new SkillsUtils(); util.assignedToRefQual(current);
```

This script has the following results.

- If an **Assignment group** is set, the list is filtered on members of that group.
- If **Skills** are set (the **Skills** field may need to be added to the form), the list is filtered on users with all the selected skills.
- If **Assignment group** and **Skills** are both set, the list is filtered on group members with the defined skills.

You can introduce the same behavior to other task tables by using the same reference qualifier.

Activate skills management

The Skills Management plugin is automatically activated by the Field Service Management and Project Management plugins. Administrators can also activate the Skills Management plugin manually.

1. Navigate to **System Definition > Plugins**.
2. Find and click the plugin name.
3. On the System Plugin form, review the plugin details and then click the **Activate/Upgrade** related link.

   If the plugin depends on other plugins, these plugins are listed along with their activation status.

   If the plugin has optional features that depend on other plugins, those plugins are listed under **Some files will not be loaded because these plugins are inactive**. The optional features are not installed until the listed plugins are installed (before or after the installation of the current plugin).

4. Optional: If available, 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 practice when you first activate the plugin on a development or test instance.

   You can also load demo data after the plugin is activated by clicking the **Load Demo Data Only** related link on the System Plugin form.

5. Click **Activate**.

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 the new role to the appropriate applications and modules.

Role required: admin

Once access has been granted to a role, all of 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 base instance, see: Base system roles.

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>
<tr>
<td>Requires Subscription</td>
<td>Indicates if users with this role must be allocated to a subscription in the Subscription form in Subscription Management to stay in compliance.</td>
</tr>
<tr>
<td></td>
<td><strong>Yes</strong></td>
</tr>
<tr>
<td></td>
<td>Chargeable user role that requires allocation of users with this role to subscriptions. These user roles display in the Associated Roles related list in the Subscription form when this user role is associated with downloaded plugins for a subscription. To learn more, see Subscription form.</td>
</tr>
<tr>
<td></td>
<td><strong>No</strong></td>
</tr>
<tr>
<td></td>
<td>Not a chargeable role.</td>
</tr>
<tr>
<td></td>
<td><strong>Unspecified</strong></td>
</tr>
<tr>
<td></td>
<td>Neither</td>
</tr>
<tr>
<td>Application</td>
<td>Select the application that contains this record.</td>
</tr>
<tr>
<td>Elevated privilege</td>
<td>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 to high security. See Elevated privilege roles for more information.</td>
</tr>
<tr>
<td>Description</td>
<td>Select the roles to delegate to the group member.</td>
</tr>
</tbody>
</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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group</td>
<td>Select a group.</td>
</tr>
<tr>
<td>Role</td>
<td>Select the role to apply to the group.</td>
</tr>
<tr>
<td>Inherits</td>
<td>Select this option to have all members of the group inherit the role. This option is selected by default.</td>
</tr>
</tbody>
</table>

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 shushbucket 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 affect 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:** The system does not support changing the name of any base system role. Changing the name of a base system role will prevent users and groups from accessing base system resources that depend on these roles.
### Base system roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>admin</strong></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 <strong>Special Administrative Roles</strong>.</td>
</tr>
<tr>
<td>agent_admin</td>
<td>Can manage MID Server-related scripts.</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>
<tr>
<td>category_manager</td>
<td>Can create, edit, and delete model categories.</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>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>Role</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</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>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>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>Role</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</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 <a href="#">Create an ACL rule</a>. 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>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>Role</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</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>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>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_admin</td>
<td>Can create and modify templates.</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>Role</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ts_admin</td>
<td>Can administer <em>Zing text indexing and search engine.</em></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:** The system does not support changing the name of any special administrative role. Changing the name of a special administrative role will prevent users and groups from accessing base system resources that depend on these roles.

**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 <em>Assignment Rules.</em></td>
</tr>
<tr>
<td>ui_script_admin</td>
<td>Allows management of UI Scripts.</td>
</tr>
<tr>
<td>script_include_admin</td>
<td>Can manage <em>Script Includes.</em></td>
</tr>
<tr>
<td>ui_page_admin</td>
<td>Can manage <em>UI Pages.</em></td>
</tr>
<tr>
<td>ui_macro_admin</td>
<td>Can manage <em>UI Macros.</em></td>
</tr>
<tr>
<td>form_admin</td>
<td>Can manage Forms, and Form Sections and Section Elements.</td>
</tr>
<tr>
<td>business_rule_admin</td>
<td>Can manage <em>Business Rules.</em></td>
</tr>
<tr>
<td>client_script_admin</td>
<td>Can manage <em>Client Scripts.</em></td>
</tr>
<tr>
<td>ui_policy_admin</td>
<td>Can manage UI Policies.</td>
</tr>
<tr>
<td>ui_action_admin</td>
<td>Can Manage <em>UI Actions.</em></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 can 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 as a simple way to limit access to data without having to create ACLs for system and 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

For evaluation, you can activate the plugin for an application that requires a purchased subscription on a non-production instance. To activate the plugin on production instances, you must purchase the subscription. To purchase a subscription, contact your ServiceNow account manager. For details on purchasing a plugin, see Purchase a plugin.

Some plugins require activation by ServiceNow personnel. Request these plugins through the HI Customer Service System instead of activating them yourself. For details, see Request a plugin.

For plugins that you can activate yourself, continue with the following steps.

1. Navigate to System Definition > Plugins.
2. Find and click the plugin name.
3. On the System Plugin form, review the plugin details and then click the Activate/Upgrade related link.

If the plugin depends on other plugins, these plugins are listed along with their activation status.

If the plugin has optional features that depend on other plugins, those plugins are listed under Some files will not be loaded because these plugins are inactive. The optional features are not installed until the listed plugins are installed (before or after the installation of the current plugin).
4. Optional: If available, 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 practice when you first activate the plugin on a development or test instance.

You can also load demo data after the plugin is activated by clicking the **Load Demo Data Only** related link on the System Plugin form.

5. 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>
<tbody>
<tr>
<td>glide.security.snc_read_only_role.tables.exempt_create</td>
<td>Specifies which tables are exempt from the read-only role enforcement and allow the creation of new records.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• 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</td>
</tr>
<tr>
<td></td>
<td>• Location: System Properties (sys_properties) table</td>
</tr>
<tr>
<td>glide.security.snc_read_only_role.tables.exempt_write</td>
<td>Specifies which tables are exempt from the read-only role enforcement and allow the updating of existing records.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• 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</td>
</tr>
<tr>
<td></td>
<td>• Location: System Properties (sys_properties) table</td>
</tr>
<tr>
<td>glide.security.snc_read_only_role.tables.exempt_delete</td>
<td>Specifies which tables are exempt from the read-only role enforcement and allow the deletion of existing records.</td>
</tr>
<tr>
<td></td>
<td>• Type: string</td>
</tr>
<tr>
<td></td>
<td>• Default value: sys_user_preference, sys_ui_list, sys_ui_list_element, sys_db_cache, user_multifactor_auth</td>
</tr>
<tr>
<td></td>
<td>• Location: System Properties (sys_properties) table</td>
</tr>
</tbody>
</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.
Role delegation

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:**
- Plugin Required
- Functionality described here requires the Security Jump Start (ACL Rules) plugin. 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>Name</td>
<td>Operation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</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>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>Name</td>
<td>Operation</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</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 to 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>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>Name</td>
<td>Operation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</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>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>Name</td>
<td>Operation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>sys_security_type</td>
<td>create</td>
<td>admin role required to create Security Type records</td>
</tr>
<tr>
<td></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></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></td>
<td>create</td>
<td>template_editor role required to create Template records</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td>template_editor role required to delete Template records</td>
</tr>
<tr>
<td></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></td>
<td>delete</td>
<td>admin role required to delete UI Action records</td>
</tr>
<tr>
<td></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></td>
<td>create</td>
<td>admin role required to create UI View Action records</td>
</tr>
<tr>
<td></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></td>
<td>delete</td>
<td>admin role required to delete UI Policy records</td>
</tr>
<tr>
<td></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></td>
<td>delete</td>
<td>admin role required to delete UI Policy Action records</td>
</tr>
<tr>
<td></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></td>
<td>delete</td>
<td>admin role required to delete UI 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_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_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 write to 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>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>

**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>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</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 HI.

- 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, connect through single-sign-on, or be used as a MID Server 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

All users with the 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>Chart or report</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</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>
</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.
- Refresh, Configure, or Close 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.

© 2019 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.
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.

<table>
<thead>
<tr>
<th>Authentication methods</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local database</td>
<td>The username and password in their user record in the instance database.</td>
</tr>
<tr>
<td><strong>External Single Sign-on (SSO)</strong></td>
<td>The username and password configured in identity providers, which have a matching user account in the database.</td>
</tr>
<tr>
<td>LDAP</td>
<td>The 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>The username and password of OAuth identity provider, which has a matching user account in the database.</td>
</tr>
<tr>
<td>Digest Token</td>
<td>An encrypted digest of the username and password in the user record.</td>
</tr>
<tr>
<td>Multifactor</td>
<td>The username and password in the database and a passcode sent to the user’s mobile device that has Google Authenticator installed.</td>
</tr>
</tbody>
</table>

Note: The OKTA SSO plugin has been deprecated for the London release. It is still available in Jakarta.

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
- 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.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 [saml2_update1_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>
<tr>
<td>SSO Federation [sso_federation]</td>
<td>Stores data for each SSO federation.</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>
</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 Definition > Plugins**.
2. Find and click the plugin name.
3. On the System Plugin form, review the plugin details and then click the **Activate/Upgrade** related link.
   - If the plugin depends on other plugins, these plugins are listed along with their activation status.
   - If the plugin has optional features that are not functional because other plugins are inactive, those plugins are listed. A warning states that some files are not installed. If you want the optional features to be installed, cancel this activation, activate the necessary plugins, and then return to activating the plugin.
4. Optional: If available, 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 you first activate the plugin on a development or test instance.
   - You can also load demo data after the plugin is activated by clicking the **Load Demo Data Only** related link on the System Plugin form.
5. Click **Activate**.

### 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-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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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_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>
Multi-SSO (SAML) IdP authentication flow

Access SNC Instance

Multi-SSO enabled?

Yes

SAML SSO Cookie exist?

Yes

IdP used to create cookie

No

Auto-redirect IdP?

Yes

Auto-redirect IdP

No

Federated IdP

Federation:xxx

Is IdP sso:xxx or federation:xxx

Yes

IdP specified on SSO source?

Yes

Does user exist?

Yes

User Auto-provisioning IdP?

No

Active default IdP?

Yes

Auto-provisioning IdP

No

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.

**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 white list.

Role required: admin

1. Navigate to Multi-Provider SSO > 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.
6. Click **Save**.

7. Instruct your users to click the **Use external login** link when they log in to 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></td>
<td></td>
<td><strong>Note:</strong> The option to set this property only comes after a successful test connection.</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></td>
<td></td>
<td><strong>Note:</strong> If you make a new Auto Redirect IdP configuration active, the <code>glide_sso_id</code> cookie updates with the new Auto Redirect IdP. The <code>glide.authenticate.sso.update.idp.cookie</code> system property, automatically enabled, controls this feature.</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>
<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>Property</td>
<td>Required</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------</td>
<td>------------------------------------------------------------------------------</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.servicenow.com/navpage.do">https://yourinstance.servicenow.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.servicenow.com/">https://yourinstance.servicenow.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.servicenow.com/">https://yourinstance.servicenow.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

![Encryption And Signing Tab](image)
## Encryption And Signing fields

<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.</td>
</tr>
<tr>
<td></td>
<td>The metadata generated for the IdP embeds the x509 certificate, which the IdP</td>
</tr>
<tr>
<td></td>
<td>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 tab](image)

### 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>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>Property</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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 a certificate is no longer valid, the system automatically polls the IdP for a current, valid certificate. 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.
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.
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:
### Option Description

**Multi-Provider SSO**
Navigate to Multi-Provider SSO > 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.

**SAML 2 SSO**
Navigate to SAML 2 Single Sign-on > Metadata.
The integration automatically generates the instance's SP metadata from the system property settings.

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" />
    <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
- AudienceRestriction/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.
Common IdP connection errors
The following table describes some of the common IdP connection errors and their solutions.

<table>
<thead>
<tr>
<th>Error messages</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Field validation failed. Invalid User Field ‘&lt;field name&gt;’ is not a field on sys_user 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 Identity Provider URL contains a valid URL to your IdP. Each IdP URL must be unique.</td>
</tr>
<tr>
<td>AudienceRestriction validation failed.</td>
<td>Verify the Audience URI contains a valid URL to your instance.</td>
</tr>
<tr>
<td>Cannot logout of IdP’s session.</td>
<td>Verify the SingleLogoutRequest URL 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>
</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. |
| • Unable to locate SAML 2.0 certificate.  
• Could not find a digital signature stored in the ServiceNow instance. | Ensure that the IDP x509 certificate is present, valid, and active | The PEM-formatted string should be entered into the PEM Certificate field. | The SAML certificate does not exist. It might be inactive. | • Ensure that the correct PEM-formatted certificate is uploaded to the instance.  
• Verify that the certificate has the name SAML 2.0. No other names are allowed. |

Note: This naming convention is only applicable for the SAML2 update 1 plugin.
<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>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>
<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: <code>&lt;inResponseTo&gt;</code>, actual: <code>&lt;inResponseTo&gt;</code></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: <code>&lt;message&gt;...</code></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>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>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. The StatusCode in the response would contain Responder instead of the expected Success.</td>
<td>Review SAMLResponse to determine if Conditions are included in the SAMLResponse. The valid subject confirmation data could be expired or not for the right audience.</td>
</tr>
<tr>
<td>Assertion audience mismatch. Expect: <code>&lt;propAudience&gt;</code>, actual: <code>&lt;audienceUrl&gt;</code>. or AudienceRestriction validation failed. No matching audience found.</td>
<td>Ensure that the 'Audience URI' field is set correctly</td>
<td>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. • 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> or 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 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.</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 is valid in the future, now: <code>&lt;now&gt;</code>&lt;br&gt;notBefore: <code>&lt;notBefore&gt;</code> or&lt;br&gt;Assertion is expired, now: <code>&lt;now&gt;</code>&lt;br&gt;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>
<tbody>
<tr>
<td>Login requests generate an infinite loop between the system and the IdP when High Security is active.</td>
<td>• Typically the URL endpoint is an error page or logout page.&lt;br&gt;• 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.</td>
<td>Set (or create) the system property glide.authenticate.failed_redirect to redirect failed authentication requests to this URL.</td>
</tr>
<tr>
<td>The token used to authenticate the user or the request is signed with the signature algorithm <a href="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256">http://www.w3.org/2001/04/xmldsig-more#rsa-sha256</a> which is not the expected signature algorithm <a href="http://www.w3.org/2000/09/xmldsig#rsa-sha1">http://www.w3.org/2000/09/xmldsig#rsa-sha1</a>.</td>
<td>Check the Alert Context tab for event details.</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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 ESS pages with Multi-Provider SSO**

You can redirect ESS users to an employee self-service page by adding a system property.

**Role required:** admin
You can add a global property to the system properties table. It applies to all IdPs. You cannot set multiple values for different IdPs.

1. Add the following system property: `glide.entry.loggedin.page_ess`.
2. Set the value of this property to the ESS page name: `myesspages`.
   If the user has no role, they are redirected to that URL. If the user has a role, they are redirected to `instance.service-now.com/navpage.do`.

**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. To 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>Assertion Consumer URL for eSignature authentication</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>Assertion Consumer Index for eSignature authentication</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>AuthnRequest URL for eSignature Authentication</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>Authentication Pop-up Dialog Width</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>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 Definition > Plugins**.
2. Find and click the plugin name.
3. On the System Plugin form, review the plugin details and then click the **Activate/Upgrade** related link.

   - If the plugin depends on other plugins, these plugins are listed along with their activation status.

   - If the plugin has optional features that depend on other plugins, those plugins are listed under **Some files will not be loaded because these plugins are inactive**. The optional features are not installed until the listed plugins are installed (before or after the installation of the current plugin).

4. Optional: If available, 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 practice when you first activate the plugin on a development or test instance.

   - You can also load demo data after the plugin is activated by clicking the **Load Demo Data Only** related link on the System Plugin form.

5. Click **Activate**.

**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 master 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 master 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.

<table>
<thead>
<tr>
<th>Secure LDAP connections</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connection</strong></td>
</tr>
<tr>
<td>MID Server</td>
</tr>
<tr>
<td>LDAPS</td>
</tr>
<tr>
<td>VPN</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 Create a transform map.

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 Upload 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.
Upload the LDAP X.509 SSL certificate
If your administrator is setting up an SSL-encrypted LDAP integration (LDAPS) to communicate over TCP on port 636, and has not already uploaded a certificate as part of your instance Go Live activities.

Role required: admin
1. Purchase or generate an SSL certificate on your LDAP server.
2. Upload the LDAP certificate to the instance.

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](image)

<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>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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 |
| Login password                | Enter the server’s password.                                                                                                                                                                                |
| Starting search directory     | Enter the relative distinguished name (RDN) of the default search directory. All queries to this LDAP server will start from this RDN.                                                                      |
| MID Server                    | 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.  
  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 |
<p>| Connect timeout               | 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.                                                         |
| Read timeout                  | 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. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td>Note:</td>
<td>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.</td>
</tr>
<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>
<tr>
<td>Note:</td>
<td>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.</td>
</tr>
</tbody>
</table>

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>
</tr>
</thead>
</table>
| glide.ldap.listener.use_background_transaction | 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.  

**Note:** 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. |

- Type: true | false
- Default value: false
- Location: Add to the System Property (sys_properties) table |

© 2019 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>
</tr>
</thead>
<tbody>
<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>
</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>
</tr>
</tbody>
</table>

**Note:** 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.

- **Type:** true | false
- **Default value:** false
- **Location:** Add to the System Property (sys_properties) 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 an 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 CN=Users,DC=service-now,DC=com and any directory below this point. This field must match a subdirectory in your LDAP system.</td>
</tr>
</tbody>
</table>
| Query field | 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 `sAMAccountName` attribute. Other LDAP servers tend to use the `cn` 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 joe.example, there must be a user record with a User ID value of `joe.example` and an LDAP record with an sAMAccountName value of `joe.example`. |
<p>| Active    | Select this check box to activate the OU definition and to allow administrators to test importing data. However, the integration can only bring data into the system from active OU definitions. |
| Table     | Specify the table that receives the mapped data from your LDAP server. For users, select User (sys_user), and for groups, select Group (sys_group). |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>Enter an LDAP filter string to select specific records to import from the OU. The more specific the LDAP filter query, the more efficient the query is. For example, the Users LDAP OU definition uses the following filter to select records that are classified as a person, have an sn attribute value, are not computers, and are not flagged as inactive: <code>(&amp;{objectClass=person}(sn=*)) (!{objectClass=computer}) (!{userAccountControl:1.2.840.113556.1.4.803:=2})</code> You can find a description of LDAP filter syntax by searching the internet for LDAP Filters RFC.</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:

<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>
</tbody>
</table>
### LDAP property

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.ldap.user.autoprovision</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 facilitates communication and movement of data between the platform and external applications, data sources, and services. For details on installing a MID Server, see [MID Server installation](#).

You can use the MID Server to import data over LDAP, but you cannot use the MID Server for LDAP authentication. A MID Server does not support SSL connections.

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 data centers.

**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
  - Using the UI action **Refresh from LDAP** 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).

An instance can connect to an LDAP server via the MID Server. When you do this, the instance communicates with the MID Server via HTTPS, and the MID Server communicates with the LDAP server via LDAP (port 389). The instance can also connect to the LDAP server directly, using LDAP or LDAPS, either over the internet or through a VPN tunnel.

**Note:** LDAP cannot communicate via the MID Server with password authentication.

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

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.

![Test Connection](image)

**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.

<table>
<thead>
<tr>
<th>Created</th>
<th>Agent</th>
<th>Topic</th>
<th>Name</th>
<th>Source</th>
<th>Queue</th>
<th>State</th>
<th>Processed</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013-07-29 13:09:36</td>
<td>mid_server.local_mid</td>
<td>LDAPProbe</td>
<td></td>
<td>output</td>
<td>processed</td>
<td>2013-07-29 13:09:46</td>
<td></td>
</tr>
</tbody>
</table>

**Import Load**

Also keep an eye out for an output message called LDAPProbeError.

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 Coalesce 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.
Default LDAP transform maps

<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>
<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.

<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>
### 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>phone</td>
<td>telephoneNumber</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 includes 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:

```javascript
// 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.

```javascript
// 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
```
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.

**LDAP monitor**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh</td>
<td>You can configure the refresh rate by clicking the Refresh field in the LDAP Server Monitor header bar, and selecting the number of seconds between each data refresh. You can also select None to suppress refreshing.</td>
</tr>
<tr>
<td>Connection Status</td>
<td>The server connection indicator is located on the right side, above the LDAP Listener Status fields. When the server is connected, the box is green and shows Connected. When the server is not connected, the box is red and shows Not Connected. When the server connection is being tested, the box is yellow and shows Testing Connection.</td>
</tr>
<tr>
<td>LDAP Server Properties</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Edit</td>
<td>As you monitor LDAP servers, you can make changes to the properties by clicking Edit in the LDAP Server Monitor screen.</td>
</tr>
<tr>
<td>Server URL</td>
<td>The combination of the server name and server port where the LDAP Server is listening. Frequently, the port is set to one of the following: • 389: the default port for connecting to LDAP in clear text • 636: the standard port for connecting to LDAP via an SSL connection Example value: ldap://10.10.3:389/ Your LDAP Server may have more than one URL address. This does NOT establish multiple directory structures from which you can import data, which is done by creating another LDAP Server entry, but does provide for redundancy when you have multiple LDAP Servers to avoid a single point of failure. The LDAP URL addresses are separated with a space character, and the system automatically tries each server address in turn until a valid connection can be made.</td>
</tr>
<tr>
<td>Starting search directory</td>
<td>The starting directory or RDN (Relative Distinguished Name) where the system begins searching for users or groups. Example value: DC=service-now,DC=com No data ABOVE this point is available for import. The instance has visibility into the specified directory and directories BELOW it in the LDAP hierarchy.</td>
</tr>
<tr>
<td>MID Server Status</td>
<td>The current connection status of the MID Server.</td>
</tr>
<tr>
<td>LDAP Listener Status</td>
<td>Current Status This indicates whether the listener is active.</td>
</tr>
<tr>
<td></td>
<td>Last Info Message This shows the last message the LDAP server received relating to user and group changes, and the time the message was received.</td>
</tr>
<tr>
<td></td>
<td>Last Change This shows the last change made to the LDAP server, and the time it was made.</td>
</tr>
<tr>
<td></td>
<td>Last Error This shows the last error that occurred on to the LDAP server, and the time it occurred.</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>Not used</td>
<td></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></td>
<td>Not used.</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></td>
<td>Not used.</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>Error / data code</td>
<td>Text</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------------</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>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>Error / data code</td>
<td>Text</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>------</td>
<td>-------------</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>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>Error / data code</td>
<td>Text</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</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></td>
<td>Not used.</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>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>Error / data code</td>
<td>Text</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</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></td>
<td>Not used.</td>
</tr>
<tr>
<td>80</td>
<td>LDAP_OTHER</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>
</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>Error / data code</td>
<td>Text</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------</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.
   ```plaintext
   (&(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.
   ```plaintext
   (&(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;
    target.locked_out = true;

    // Ignore any insert of a disabled record
    if (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";
}
*/
onBefore transform map script

Here is an example of a 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;
}
```

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 Server 2008. A download is available at [http://www.microsoft.com/downloads](http://www.microsoft.com/downloads) for earlier operating systems.

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 `adaminstall.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>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 <code>dc=myCompany,dc=com</code>, you could create the ADAM partition as <code>dc=myCompany,dc=adam</code>.</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. DSALCS is used to view and set object access rights.

Example: `dsacls \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. DSACLS is a complex tool used to create complex delegation. Run "DSACLS /?" 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. Transitively 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>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</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>
<tr>
<td>/S</td>
<td>Web site ID to attach the certificate to</td>
</tr>
<tr>
<td>/P</td>
<td>IP port of the web service</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 **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 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 ADAMSync.

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 -->
  <!-- source-ad-name = fqdn of the domain controller -->;
  <!-- source-ad-partition = root AD domain partition -->;
  <!-- target-dn = target ADAM OU -->;
  <!-- base-dn = should be the root AD partition if you want all users -->;
  <!-- object-filter = standard ldap query format, this will grab all users -->;
  <!-- need to review results to see if you should modify this filter -->;
  <!-- include=userproxy requires objectSID to link back to the AD account -->;
  <description>MyCompany ADAMSConfig Configuration</description>
  <security-mode>object</security-mode>;
  <source-ad-name>;fully.qualified.domain.name.of.domain.controller</source-ad-name>;
  <source-ad-partition>;dc=myCompany,dc=com</source-ad-partition>;
  <source-ad-account>;</source-ad-account>;
  <account-domain>;</account-domain>;
  <target-dn>;ou=servicenow users,dc=myCompany,dc=adam</target-dn>;
  <base-dn>;dc=myCompany,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>;sAMAccountName</include>;
  </attributes>;
</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 &
- **OR** = "|" (vertical line) replace with |
- **NOT** = "!" replace with !

Reference configuration file

Here's an actual configuration file that can be referenced as a sample.

```xml
<?xml version="1.0"?>;
<configuration>;
<description>;SNCTest ADAMSync Configuration</description>;
<security-mode>;object</security-mode>;
<source-ad-name>;domaincontroller.service-now.com</source-ad-name>;
<source-ad-partition>;domaincontroller.service-now.com</source-ad-partition>;
<source-ad-account>;domaincontroller.service-now.com</source-ad-account>;
<account-domain>;domaincontroller.service-now.com</account-domain>;
<target-dn>;ou=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>
```
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 CertSrv 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>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>E-Mail</td>
</tr>
<tr>
<td>Company</td>
</tr>
<tr>
<td>Key Options settings</td>
</tr>
<tr>
<td>Create new key set</td>
</tr>
<tr>
<td>Field</td>
</tr>
<tr>
<td>-----------------------------------</td>
</tr>
<tr>
<td>CSR</td>
</tr>
<tr>
<td>Key Usage</td>
</tr>
<tr>
<td>Key Size</td>
</tr>
<tr>
<td>Automatic key container name</td>
</tr>
<tr>
<td>Store certificate in the local computer certificate store</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 that 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 Upload 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 ServiceNow Technical 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.

   ```
   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.

   ```
   objectclass ( 1.3.6.1.4.1.3403000.2.2.1
     NAME 'BcfUserIdentifiers' SUP top AUXILIARY
   ```
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.

**SAML 2.0**

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 high security property by selecting System Security > High Security Settings.

**Note:** It is recommended that customers using an existing SAML 2.0 integration upgrade to the latest Multi-Provider SSO plugin.

**Activate and set up SAML 2.0**

SAML 2.0 activates through the Integration - Multiple Provider Single Sign-On Installer plugin.
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 Definition > Plugins.
2. Find and click the plugin name.
3. On the System Plugin form, review the plugin details and then click the Activate/Upgrade related link.
   - If the plugin depends on other plugins, these plugins are listed along with their activation status.
   - If the plugin has optional features that depend on other plugins, those plugins are listed under Some files will not be loaded because these plugins are inactive. The optional features are not installed until the listed plugins are installed (before or after the installation of the current plugin).
4. Optional: If available, 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 practice when you first activate the plugin on a development or test instance.
   - You can also load demo data after the plugin is activated by clicking the Load Demo Data Only related link on the System Plugin form.
5. Click Activate.

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
Note: When you create the clone, include attachments so that certificates carry over to the target instance. Also, make sure the Theme check box is cleared so these properties are preserved regardless of whether you preserve the instance theme.

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:

```xml
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    Destination="https://demo12.service-now.com/navpage.do"
    ID="s28da6774c88ae1eab292bf25fe625db81919d8e1e"
    InResponseTo="SNC841720c227c81948cf6d8cadcad235c6"
    IssueInstant="2012-01-30T07:10:02" Version="2.0">
    ...
    <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
        ID="s2f347f973c063836cf70ea38302d94976f9c5b851"
        IssueInstant="2012-01-30T07:10:02" Version="2.0">
        ...
    </saml:Assertion>
</samlp: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 following property, enter the URL obtained from the SingleLogoutService element: The base URL to the Identity Provider's SingleLogoutRequest service. The LogoutRequest will be posted to this URL as the SAMLRequest parameter. The LogoutRequest is posted to this URL as the SAMLRequest parameter.

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.**

Example third-party SAML identity provider (IdP) configuration
View a video showing a third-party SAML IdP configuration.

An instance does not typically provide instructions for configuring third-party SAML IdP products, but customers might occasionally provide examples of how they have implemented their SAML IdP with their instance.

**Note:** The instance does not provide support for example configurations.

## IdP setup configuration

<table>
<thead>
<tr>
<th>Identity Provider</th>
<th>Example Setup</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSOCircle</td>
<td>SSOCircle (Video Tutorial)</td>
</tr>
</tbody>
</table>

**Service Provider (SP) system properties**
These system properties define how the instance interacts with the IdP as a Service Provider.
Service Provider (Service-Now) properties

The URL to the Service-now instance homepage.
https://yourinstance.service-now.com/navpage.do

The entity identification, or the issuer
https://yourinstance.service-now.com

The audience uri that accepts SAML2 token. (Normally, it is your instance URL. For example: https://demo.service-
now.com.)
https://yourinstance.service-now.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:

```xml
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  ID="s2cdc74f37f923e26felaaecc42b70a93d24230334f"
  InResponseTo="90AA6073P01567BFB0DF194F596314E2"  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: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 URI. 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 IdPs 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>
<tr>
<td>Kerberos-based authentication</td>
<td>urn:federation:authentication:windows</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.
   
   `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`

(Optional) Advanced SAML properties

The following advanced settings allow you to further increase security and debug the integration.

**Advanced settings**

<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 <strong>Yes</strong> 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 identify 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><strong>Field</strong></th>
<th><strong>Value</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>SANL 2.0</td>
</tr>
<tr>
<td><strong>Format</strong></td>
<td>PEM</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Trust Store Cert.</td>
</tr>
<tr>
<td><strong>Valid from</strong></td>
<td>2011-05-17 12:57:21</td>
</tr>
<tr>
<td><strong>Expires</strong></td>
<td>2016-08-17 12:57:21</td>
</tr>
<tr>
<td><strong>Short description</strong></td>
<td>idp.sso.crc.de.com</td>
</tr>
<tr>
<td><strong>Issuer</strong></td>
<td>CN=CA, O=SSO Crc, C=DE</td>
</tr>
<tr>
<td><strong>Subject</strong></td>
<td>CN=Idp.sso.crc.de.com, OU=Idp, O=SSO Crc, C=DE</td>
</tr>
<tr>
<td><strong>PEMCertificate</strong></td>
<td>3a2... (content truncated)</td>
</tr>
</tbody>
</table>

**Related Links**
- Validate Store/Certificates

© 2019 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 SAML 2.0 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 PEM 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

<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, enter `sys_properties.list` in the application filter. The list of system properties opens.

5. Find and open the following property: **glide.authenticate.sso.saml2.keystore**.

   The Value field shows the Sys ID of the default key store: **SAML 2.0 SP Keystore**. Use this property when the system has multiple key stores for signed authentication or signed logout. Starting with Geneva patch 7, this property uses your configured key store if you upgrade from a version prior to the Geneva release. Prior to the Geneva patch 7, this property kept the default value upon upgrade, regardless of any changes you made.

6. Paste the Sys ID of the key store record that you created into the **Value** field.

7. 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>
<tbody>
<tr>
<td>NotAfter: &lt;Thu Jun 05 22:57:44 PDT 2014&gt;.</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. • Update the SAML 2.0 certificate record.</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>
| • Unable to locate SAML 2.0 certificate.  
• Could not find a digital signature stored in the ServiceNow instance. | Ensure that the IDP x509 certificate is present, valid, and active | The PEM-formatted string should be entered into the PEM Certificate field. | The SAML certificate does not exist. It might be inactive. | • Ensure that the correct PEM-formatted certificate is uploaded to the instance.  
• Verify that the certificate has the name SAML 2.0. No other names are allowed. |

**Note:** This naming convention is only applicable for the SAML2 update 1 plugin.

| Certificates do not match. Expect: <certStr>, actual: <inboundCert>. | Ensure that the IDP x509 certificate is present, valid, and active. | N/A | The available certificate in SNC does not match the certificate in assertion. Causes include:  
• The certificate is updated on the IdP but not in the ServiceNow instance.  
• The certificate is in the wrong format. | Confirm that the PEM-formatted string in the SAML 2.0 certificate record matches the X509 Certificate in the SAMLResponse for the user IdP. |

| Failure to check the validity of the certificate. | Ensure that the IDP x509 certificate is present, valid, and active. | N/A | The current certificate might have expired. | Update the SAML 2.0 certificate record. |

<p>| Failure to validate signature profile. | Ensure that the IDP x509 certificate is present, valid, and active. | N/A | The assertion might be signed with a different certificate. | Check if the IdP has the same certificate as the SNC instance. |</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>
</table>
| InResponseTo attribute in SubjectConfirmationData mismatch. Expect: <inResponseTo>, actual: <inResponseTo>. | Subject confirmation validation failed. | N/A            | This error appears if either of the following situations occurs:  
- The IdP returns a SAMLResponse for a different SAMLRequest  
- A user bookmarks the URL with the SAMLRequest instead of just the instance URL  
- If a null value is expected, the response might be sent to a different node when the instance has multiple nodes. | The IdP admin should confirm that the expected SAMLResponse is being returned. This situation can be a load balancer or infrastructure issue. |
| SessionIndex value not found: <message>...                                            | SessionIndex not valid. | N/A            | The **SessionIndex** is required in the SNC instance. The IdP returns it in the SAML response to authenticate successfully.  
- Conditions could be missing due to an error on the IdP.  
- The **_StatusCode** in the response would contain **Responder** instead of the expected **Success**. | The IdP admin should confirm that the **SessionIndex** is defined in the SAMLResponse.  
- Review SAMLResponse to determine if **Conditions** are included in the SAMLResponse.  
- The valid subject confirmation data could be expired or not for the right audience. |
| No valid SubjectConfirmation found.                                                   | Subject confirmation validation failed. | N/A            |         |                                                                                                                                                                                                 |                                                                                                                                                                                                                     |
| Assertion audience mismatch. Expect: <propAudience>, actual: <audienceUri>. or AudienceRestriction validation failed. No matching audience found. | Ensure that the 'Audience URI' field is set correctly | N/A            | The SNC instance configured audience URI must match the value in the IdP.  
- The **Audience URI** that accepts the SAML2 token. (Normally, it is your instance URL. For example: https:// demo.service-now.com.) | Locate `<saml2:Audience>` in the SAMLResponse in the logs and verify that the value matches the one on the instance. |

© 2019 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>
</table>
| Assertion issuer is invalid. Expect: <value on instance>, actual: <value returned by IdP> | Assertion issuer is invalid. | The Identity Provider URL that issues the SAML security token with user info. | The IdP entity id (issuer) does not match the value defined in the SNC instance. | • 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: <now>, NotBefore: <notBefore> | 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. | 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. |
| or Subject is expired. Now: <now>, NotOnOrAfter: <notOnOrAfter> | | | | |
| Assertion is valid in the future, now: <now>, notBefore: <notBefore> | 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. | 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. |
| or Assertion is expired, now: <now>, notOnOrAfter: <notOnOrAfter> | | | | |

### 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. |
<table>
<thead>
<tr>
<th>Error or Symptom</th>
<th>Diagnosis</th>
<th>Fix</th>
</tr>
</thead>
<tbody>
<tr>
<td>The token used to authenticate the user or the request is signed with the signature algorithm <a href="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256">http://www.w3.org/2001/04/xmldsig-more#rsa-sha256</a> which is not the expected signature algorithm <a href="http://www.w3.org/2000/09/xmldsig#rsa-sha1">http://www.w3.org/2000/09/xmldsig#rsa-sha1</a>.</td>
<td>Check the Alert Context tab for event details.</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Force single sign-on login (SSO) only**

When single sign-on is enabled, you might not want users to see the login page or allow user to log in locally.

In other words, if a user attempts to go to `https://customerX.service-now.com`, the internal company portal should be displayed instead of the default login page. Likewise, when a user logs out of the application, the browser should redirect them to a specific internal page. You can set redirection properties within the instance to ensure that users see the single sign-on page rather than the default login page.

**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.
Forcing login using SSO only

<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</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 <code>&lt;user_id&gt;</code>. 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:

```
var r = new Packages. java.util.Random();

var str1 = Packages. java.lang.Long.toString(Packages. java.lang.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.

![Single Sign-on Logic Flow Chart]

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" 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:

```
```
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.
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"
        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 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.

```java
return "failed_missing_requirement:%26amp;TARGET=https://instance.service-now.com/nav_to.do?uri=incident.do?sys_id=12345";
```

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.

### Properties

The SAML 2.0 Update 1 plugin includes the following system properties.
### Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Identity Provider URL which will issue the SAML2 security token with user info.</td>
<td>Enter the value of the Issuer element that the integration uses to validate the IdP URL. Each IdP URL must be unique.</td>
</tr>
<tr>
<td>glide.authenticate.sso.saml2.idp</td>
<td></td>
</tr>
<tr>
<td>Sign LogoutRequest. Set this property to true if the Identity Provider's SingleLogoutRequest service requires signed LogoutRequest.</td>
<td>Select whether the IdP requires a signed logout request.</td>
</tr>
<tr>
<td>glide.authenticate.sso.saml2.require_signed_logoutrequest</td>
<td></td>
</tr>
<tr>
<td>Select whether the IdP requires a signed logout request.</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>glide.authenticate.external.logout_redirect</td>
<td></td>
</tr>
<tr>
<td>The audience URI that accepts SAML2 token. (Normally, it is your instance URI. For example: https://&lt;instance name&gt;.service-now.com.)</td>
<td>Enter the value of the Audience element that integration uses to validate the SP URL in the SAMLResponse.</td>
</tr>
<tr>
<td>glide.authenticate.sso.saml2.audience</td>
<td></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 Yes, 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 AuthnRequest to the Identity Provider</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>glide.authenticate.sso.saml2.authncontextclassref</td>
<td></td>
</tr>
<tr>
<td>The alias of key entry stored in SAML 2.0 SP Keystore used to sign SAML 2 requests.</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>glide.authenticate.sso.saml2.signing_key_alias</td>
<td></td>
</tr>
<tr>
<td>The password of key entry stored in SAML 2.0 SP Keystore used to sign SAML 2 requests.</td>
<td>Enter the password for the key that signs SAML 2 logout requests.</td>
</tr>
<tr>
<td>glide.authenticate.sso.saml2.signing_key_password</td>
<td></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 notBefore and notOnOrAfter date-time values.</td>
</tr>
<tr>
<td>glide.authenticate.sso.saml2.clockskew</td>
<td></td>
</tr>
</tbody>
</table>
### Property | Description
---|---
**AuthnRequest URL for eSignature Authentication.**
com.snc.integration.saml_esig.idp_authnrequest_url | Enter the URL that points to the SAML 2.0 Identity Provider AuthnRequest Consumer for eSignature Authentication. In most cases, this will be the same as the AuthnRequest URL used in general authentication. Leave this setting blank if you intend to use the same AuthnRequest Consumer URL that is used for general SAML 2.0 authentication in your instance.

**The SAML 2.0 Assertion Consumer URL for eSignature authentication.**
com.snc.integration.saml_esig.approval_consumer_url | In most cases, this URL will be: https://YOURINSTANCE.service-now.com/consumer.do. However, if you employ a customized method of handling the SAML authentication for eSignature, you can set up your own consumer URL.

**The SAML 2.0 Assertion Consumer Index for eSignature authentication.**
com.snc.integration.saml_esig.assertion_consumer_service_index | 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.

**Authentication Pop-up Dialog Width.**
com.snc.integration.saml_esig.popup_dlg_width | When a user approves a request using eSignature, a dialog allows the user to enter their credentials. This setting controls the width of that dialog box.

**Authentication Pop-up Dialog Height.**
com.snc.integration.saml_esig.popup_dlg_height | When a user approves a request using eSignature, a dialog allows the user to enter their credentials. This setting controls the height of that dialog box.

---

### 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 ServiceNow Technical 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 integrate 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. See [KB0547061](https:// servicenow.com/kb0547061) for more information.

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?uri=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=46c88ac1a9fe1981014de1c831fbcf6d`). 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**
SAML 2.0 single sign-on (SSO) supports integration with Microsoft Active Directory Federation Services (ADFS) 3.0.

For information about installing and configuring ADFS, see [Active Directory Federation Services Overview](#).

---

**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

After you set up ADFS 2.0 or 3.0, set up the 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 SAML 2.0, 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 Issue 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 to 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.
You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Get Attribute

Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

<table>
<thead>
<tr>
<th>LDAP Attribute (Select or type to add more)</th>
<th>Outgoing Claim Type (Select or type to add more)</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-Mail-Addresses</td>
<td>E-Mail Address</td>
</tr>
</tbody>
</table>

```
c: [Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"]
=> issue(store = "Active Directory",
```
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.

```xml
  c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
```
15. Click Finish.

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.
3. Configure the settings:
   - **Endpoint Type:** SAML Logout
   - **Binding:** POST
   - **URL:** `https://myadfsserver.domain.net/adfs/ls/?wa=wsignout1.0`

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 Update 1 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=lQjIVp7aRJtyPx5+2O/vgU24tbE=
  ```

- 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
  %3Fsparm_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=009f8eda0a0a0b2b0ab4eb0942234666%26sysparm_stack=incident_list.do%3Fsysparm_query=active=true&SM_USER=user_name&DE_USER=lQjIVp7aRJtyPx5+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 ServiceNow Technical 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). See Activate a plugin.

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_update1</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 new 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.

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    Destination="https://demoi2.service-now.com/navpage.do"
    ID="s28da6774c88ae1ab292bf25fe625db81919d8e1e"
    InResponseTo="SNC841720c227c81948cfd68cadcad235c6"
    IssueInstant="2012-01-30T20:07:10Z" Version="2.0">
    ...
    <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
        ID="s2f347f973c063836cf70ea38302d94976f9c5b851"
        IssueInstant="2012-01-30T20:07:10Z" Version="2.0">
        ...
    </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.

```
<saml:SubjectConfirmationMethod="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <saml:SubjectConfirmation InResponseTo="SNC841720c227c81948cfd68cadcad235c6"
</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.

```
    <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>This issue might occur in a multi-node environment. If the plugin does not get activated on all nodes, an error like the following appears: org.mozilla.javascript.EcmaError: (JavaPackage org.opensaml.saml2.core.impl.AuthnRequestBuilder) is not a function.</td>
<td></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 view_content.do public page from active=true to active=false.</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 URI to control where the user is directed after authentication at the IdP. SSO ignores relative URLs. For example, SSO cannot redirect users to a /ess relative URL. Instead, the user has to navigate to a URL such as /nav_to.do? url=/ess, which uses deep linking syntax. If you change the CMS entry page to make it private by setting view_content.do to active=false, deep linking behavior then requires a customization to the Installation Exit login script. Create a script that looks for the URI portion of the URL and constructs a RelayState 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><code>external.authentication.failed</code></td>
<td>The single sign-on requirements are not present or are missing.</td>
<td>Session ID</td>
<td></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 table</td>
<td>User ID</td>
<td></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></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>Record</th>
<th>Parameter 1</th>
<th>Parameter 2</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></td>
<td>The string, 'SAML2 LogoutResponse validation failed.'</td>
</tr>
<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><code>external.authentication.failed</code></td>
<td>The single sign-on requirements are not present or are missing.</td>
<td>Session ID</td>
<td></td>
<td>The missing authentication requirements</td>
</tr>
<tr>
<td>Event name</td>
<td>Description</td>
<td>User ID</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------</td>
<td>------------------------------</td>
<td></td>
</tr>
<tr>
<td>external.authentication.failed</td>
<td>The user does not exist in the User (sys_user) table.</td>
<td>User ID</td>
<td>The string, &quot;User does not exist&quot;</td>
<td></td>
</tr>
<tr>
<td>external.authentication.failed</td>
<td>The user is locked out.</td>
<td>User ID</td>
<td>The string, &quot;User locked out.&quot;</td>
<td></td>
</tr>
</tbody>
</table>

**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 [High Security Settings](#) 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>Concept</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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>
<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>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 authorization code grant flow 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 *password* 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 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 Definition > Plugins**.
2. Find and click the plugin name.
3. On the System Plugin form, review the plugin details and then click the **Activate/Upgrade** related link.
   - If the plugin depends on other plugins, these plugins are listed along with their activation status.
   - If the plugin has optional features that depend on other plugins, those plugins are listed under Some files will not be loaded because these plugins are inactive. The optional features are not installed until the listed plugins are installed (before or after the installation of the current plugin).
4. Optional: If available, 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 practice when you first activate the plugin on a development or test instance.
   - You can also load demo data after the plugin is activated by clicking the **Load Demo Data Only** related link on the System Plugin form.
5. Click **Activate**.

**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. Type `sys_properties.list` in the application navigator filter and then click **New**.
2. Fill out the form with the following settings:
   - **Name**: com.snc.platform.security.oauth.is.active
   - **Type**: true | false
   - **Default value**: true
3. Set the property to **true** to use OAuth 2.0.
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>Name</td>
<td>A unique name that identifies the application that you require OAuth access for.</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>
</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 **Manage OAuth tokens** for more information.

Create an **OAuth OIDC provider**
Create an OAuth OIDC provider to accept identity tokens generated by a third-party OIDC provider for inbound API calls.

Role required: admin

OIDC is not supported by our external Single Sign-On implementation. It is only intended for a REST message.

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 (AFDS, Auth0, Azure AD, Google, Okta), and then fill in the form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comments</td>
<td>Additional information to associate with the application.</td>
</tr>
<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 OIDC Provider Configuration</td>
<td>Choose the OIDC provider (AFDS, Auth0, Azure AD, Google, Okta) used for validating 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>
</tbody>
</table>

**Note:** If validation is not checked, the JTI cannot be validated, regardless if it is present in the JWT token.
2. Click Submit. The record is saved in the Application Registrries (oauth_entity) table. The system creates a record in the Application Registrries (oauth_entity) table with type External OIDC Provider. When the instance actually issues tokens and authorization codes, they are stored in the table. See Manage OAuth tokens 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>Automatically provision users</td>
<td>Check the box to enable user provisioning.</td>
</tr>
<tr>
<td>Provision data source</td>
<td>Specify and configure the data source to use to transform an OIDC token 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. When configuring the Transform mapping, the source fields are from the JWT token, the target fields are from the sys_user table.</td>
</tr>
<tr>
<td>User roles applied to provisioned users</td>
<td>Specify the user roles to apply to newly provisioned ServiceNow users.</td>
</tr>
</tbody>
</table>

Connect to a third-party OAuth provider

You can connect your ServiceNow instance to a third-party 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>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</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>Refresh Token Lifespan</td>
<td>Time, in seconds, the refresh token is valid. The default time is 8,640,0000 seconds.</td>
</tr>
<tr>
<td>Comments</td>
<td>Add any comments regarding the OAuth app.</td>
</tr>
<tr>
<td>Application</td>
<td>Application and scope containing this record.</td>
</tr>
<tr>
<td>Accessible from</td>
<td>Make this app accessible from all application scopes, or this scope only.</td>
</tr>
<tr>
<td>Active</td>
<td>Check this 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's token endpoint.</td>
</tr>
<tr>
<td>Token Revocation URL</td>
<td>The OAuth server's token revocation endpoint.</td>
</tr>
<tr>
<td>Redirect URL</td>
<td>The OAuth callback endpoint. If you leave it empty, it 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>
</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. 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'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 London
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</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`.

<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 <a href="#">Specify an OAuth profile</a>).</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` API methods `setScope` and `setGrantType`. For additional information, see [SetScope](#) and [SetGrantType](#).

### OAuth API request parameters

Access token request uses the following request parameters.
## 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.)

```bash
$ curl -d "grant_type=password&client_id=be3aeb583ace210011c15b24a43e25d8 &client_secret=client_password &username=admin&password=admin" https://instancename.service-now.com/oauth_token.do
```

**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.)

```bash
$ curl -d "grant_type=refresh_token&client_id=be3aeb583ace210011c15b24a43e25d8 &client_secret=client_password &refresh_token=w599voG89897rGVDmdp12WA681r9E5948c1CJTPi8g4HGc4NWaz62k6k1K0FMxHN40H8y0O3H` 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 <a href="https://tools.ietf.org/html/rfc6750">RFC6750</a> 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": "w599voG89897rGVDmdp12WA681r9E5948c1CJTPi8g4HGc4NWaz62k6k1K0FMxHW4",
  "access_token": "F0jh9korTyzd9kaZq2OSzjKZu53ut0l4P46Lc52m2JYHiL1c9zFAnpuyxshU9mMQ15"
}
```

**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**
   - In step one, 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

© 2019 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.
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:

```plaintext
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 Authorize access to an OAuth endpoint using auth code flow 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:

```plaintext
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 GET request from the client application to the ServiceNow instance that provides the auth code and requests the access token:

```plaintext
https://myinstance.servicenow.com/oauth_token.do?grant_type=code&code={the auth code}&redirect_uri={the_same_redirect_url}&client_id={the_same_client_identifier}
```

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 Manage OAuth tokens.
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 **OAuth implicit grants**, also known as implicit grant code flow.

**Integration support**

Authorization code flow supports the following integrations on the instance:

- Multi-SSO
- 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 **authorization code grant flow**.

**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. The list view of tokens 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.

---

**Test endpoint** would like to connect to your ServiceNow account on instance `{instance name}`

By clicking **Allow**, you allow **Test endpoint** to connect to your ServiceNow account on instance `{instance name}` and allow it to interact with records as you.

You can change this and other **account permissions** at any time.

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 London 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 an
oauth_auth.do. For example:

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:

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:

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.

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

authcode flow: ServiceNow instance as authorization server (example)
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 2.0 on both instances.

1. On one 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 another 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 set up. 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 **Create a REST message**.

   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 **Multi-SSO** is enabled. Click **Use External Login** to access the IdP login screen.
    - Your **Multi-factor Authentication** 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.
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
Revoke 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 accessing the token in the instance.

- 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.

OAuth client APIs
The OAuth client API provides methods to request and revoke OAuth tokens.

The OAuth client provides these classes:
- : Methods for requesting and revoking the refresh and access tokens.
- : Methods for handling client requests.
- : Methods for handling client responses.
- : 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:

```javascript
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 exist 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.

<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>
<tr>
<td>Email address</td>
<td>EMAIL</td>
<td>email</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=KfN4nlI86b9gefcOYLM0=</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

After enabling a digest installation exist script, configure properties for multi-prover single sign-on.

Role required: admin

If you are not using multi-provider single sign-on, configure standard single sign-on properties.

1. In the **Name** field, enter the name of the digest token.
2. In the **User** field, enter the sys_user field that contains the matching data for the incoming header.
3. In the **HTTP Digest header name** field, enter the HTTP header you generated. For example, DE_USER.
4. In the **HTTP header name field**, enter the HTTP header you generated in Step 1. For example, SM_USER.
5. In the **Secret Passphrase** field, enter the secret key to use for encoding digest keys. For example, SecretKey123.
6. In the **Failed SSO Redirect field**, enter the URL to redirect users after a failed authentication.
7. In the **External logout redirect** field, enter the URL to redirect users after a logout.
8. In the **Single Sign-on Script**, select MultiSSO_DigestedToken.
9. Click **Update**.

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=KfNr4nlt86b9gEfooiT0dU/YLM0=
  ```

- **HTTP Header Format:**
  ```
  SM_USER=joe.employee;DE_USER=KfNr4nlt86b9gEfooiT0dU/YLM0=
  ```

- **Cookie Format:**
  ```
  SM_USER=joe.employee;
  DE_USER=KfNr4nlt86b9gEfooiT0dU/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=nqQ82LONeYQnXPmqddxnsvsArrQ=
  ```

- https://demo.service-now.com/nav_to.do?uri=incident.do?
  ```
  sys_id=9d385017c611228701d22104cc95c371&SM_USER=itil&DE_USER=Uj/HopjjPczCNpN2xCXl7kQty4=
  ```

- http://demo.service-now.com/nav_to.do uri=incident_list.do?
  ```
  sysparm_userpref_module=4dedbac7d0bbf538017a7f13c41f257%26sysparm_query=caller_id=javascript:gs.getUserID()^active=true^EQ&SM_USER=itil&DE_USER=Uj/HopjjPczCNpN2xCXl7kQty4=
  ```

**Note:** If you are using request parameters inside a URL (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"; // default to something JDK 1.4 has String fKey = "abc123"; 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 (IllegalStateException e) { e.printStackTrace(); } return null; } public static void main(String[] args) { BASE64Encoder encoder = new BASE64Encoder(); DigestTest test = new DigestTest(); String userName = "user_name"; System.out.println("base 64 digest username: " + encoder.encode(test.getDigest(userName))); } }
```

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;
    }
```
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 in combination with the following authentication methods:
  - Local Database Authentication (native ServiceNow authentication)
  - LDAP integration

Authentication methods that are not supported

- MFA is not supported in combination with the following authentication methods:
  - SSO SAML
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 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 account and master password with the Chrome extension before you set up MFA with the extension.</td>
</tr>
<tr>
<td>Questions</td>
<td>Answers</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</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 multifactor authenticator**

Administrators can activate the **Integration - Multifactor Authentication plugin**, which is not active by default.

Role required: admin

1. Navigate to **System Definition > Plugins**.
2. Find and click the plugin name.
3. On the System Plugin form, review the plugin details and then click the **Activate/Upgrade** related link.

   If the plugin depends on other plugins, these plugins are listed along with their activation status.
If the plugin has optional features that are not functional because other plugins are inactive, those plugins are listed. A warning states that some files are not installed. If you want the optional features to be installed, cancel this activation, activate the necessary plugins, and then return to activating the plugin.

4. Optional: If available, 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 you first activate the plugin on a development or test instance.

You can also load demo data after the plugin is activated by clicking the **Load Demo Data Only** related link on the System Plugin form.

5. Click **Activate**.

### Configure multifactor authentication

You can enable multifactor authentication on the instance and specify how many times users can skip the additional passcode requirement.

Role required: admin

1. Navigate to **Multi-factor Authentication > Properties**.

2. Configure these properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Multifactor Authentication</td>
<td>Select this check box to allow users and administrators to use this feature.</td>
<td>Enabled</td>
</tr>
<tr>
<td>Number of times a user can bypass multifactor authentication</td>
<td>Enter a number that represents how many times a user can choose to skip the additional passcode requirement. This gives your users the ability to still log in the instance if they do not have their mobile device with them. If you disable this feature and then re-enable it, the counter starts over again.</td>
<td>3</td>
</tr>
<tr>
<td>The time in minutes, the one time code sent to user's email address is valid for</td>
<td>Enter a number in minutes that specifies how long the reset code is valid. See <strong>Log on with multifactor authentication</strong>.</td>
<td>10</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Additional time in seconds for which the code will be valid to accommodate for the clock skew. Max value is 60 seconds. (glide.authenticate.multifactor.clock_skew)</td>
<td>Enter a number in seconds with a maximum of 60. By default, the instance validates the code entered by the user against the single app-generated code generated at whatever the current time is. You can skew the time window with this property and allow one or more codes 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 generated by the app between the time range [the current time - 5 seconds] and [current time + 5 seconds] to be valid. Use this property to prevent log in issues where the user is unable to enter the correct code in the default time allotted.</td>
<td>10</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

© 2019 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.
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 multifactor authentication for a user
You can require multifactor authentication 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.

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.
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.
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 enabled 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

<table>
<thead>
<tr>
<th>1. Download the app</th>
<th>2. Scan the QR Code:</th>
<th>3. Type in the App’s response:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple iTunes</td>
<td>Google Play</td>
<td>Windows Store</td>
</tr>
</tbody>
</table>

[QR Code Image]

Or type in: KW2YUUCQ6S6IBI0EN

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 your User profile

Users can disable multifactor authentication on their own user profile.

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.

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
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. For the Jakarta release, this feature does not support sessions created through the native mobile app or non-interactive mechanisms.

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>glide.authenticate.limit.concurrent.interactive.sessions</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></td>
<td><strong>Note</strong>: To disable this feature, set this property back to <strong>False</strong>.</td>
</tr>
<tr>
<td>glide.authenticate.max.concurrent.interactive.sessions</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. |
|                                             | **Note**: Only web and mobile browser sessions can have a limit. There are no limits for sessions that originate from the ServiceNow mobile app or non-interactive sessions. |
| 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.

Associating custom URLs to your instance

You can enable your ServiceNow instance to be accessible from a company-branded or custom URL.

You can configure one or multiple custom URLs to your instance, and configure your custom URL to service portal mapping.

<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 specific configurations which must be done before you can create the custom URL on your instance:

<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>
<tr>
<td>Configuration items</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Determine your dedicated VIP status</td>
<td>Your ServiceNow instance must be on a dedicated VIP. Contact ServiceNow support for any issues.</td>
</tr>
</tbody>
</table>

**Activate Custom URL**

Enables a Custom URL 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 **Custom URL**.
   - **Note**: Do not choose **Custom URL - Internal**, which is an internal component for scripted custom URL APIs.
3. On the **System Plugin** form, click the **Activate/Upgrade** related link.
4. Click **Activate**.
   - After activation completes, choose **Close and reload form** to stay on this form.
5. Go to the **Plugin Files** tab, find the following property, and change the setting value:
   - **glide.customurl.enabled**
     - To enable custom URLs, set the value to **True**. By default, this property is set to **False**, which means you cannot associate a custom URL.
     - **Note**: To disable this feature, set this property back to **False**.
6. Click **Update** to have the settings take effect.

**Set your custom URL as the instance URL**

Add a custom URL to your instance configuration to use instead of your ServiceNow designated URL.

Role required: admin

You must have purchased or registered a URL before adding the custom URL to your instance.

1. Navigate to **Custom URL > Custom URLs**.
   - Click **New** to associate a new domain name.
   - Choose a custom URL to set as your instance.
2. Fill in the appropriate fields:
   - **Domain Name**
     - Fully qualified domain name (FQDN) of the custom URL.
     - **Note**: If the custom URL is 'https://servicenow.acme.com', enter 'servicenow.acme.com' as the FQDN.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is Instance URL</td>
<td>Checking this box enables this custom URL for all outbound URLs. Only one active custom URL can be the instance URL. To enable this setting, click the 'Set as Instance URL' button on an active custom URL. This setting activates the chosen custom URL and removes any other custom URL previously set.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the custom URL record. Once the status shows as 'Active', the custom URL is provisioned and ready to use.</td>
</tr>
<tr>
<td>(Optional) Service Portal</td>
<td>Choose the service portal to redirect users when they access your instance using the custom URL.</td>
</tr>
</tbody>
</table>

A custom URL should activate within six hours. Polling for custom URL job completion occurs every 30 minutes.

**Note:** There is a poll button for manual polling an in-progress custom URL job.

**Custom URL datacenter job information**

Every custom URL associated to your instance has a corresponding ServiceNow datacenter job which runs and shows pertinent custom URL information.

<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 of when the job last ran.</td>
</tr>
<tr>
<td>Payload</td>
<td>The 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 the results have polled for this job.</td>
</tr>
<tr>
<td>Result</td>
<td>Verifies and validates each domain or custom URL sent in 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, Okta).

1. Choose your installed SSO plugin:
ServiceNow London Now Platform Administration

<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" />
    <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 setup custom URLs in Azure:
   a) Go to App Registrations
   b) Select All apps from 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>Note: It usually takes 30 minutes to create a custom URL. If it is taking longer, contact ServiceNow Technical Support.</td>
<td></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 status on Custom URL Jobs before submitting 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 &lt;custom_domain&gt; 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>&lt;custom_domain&gt; is now the instance URL. &lt;base.service-now.com&gt; is still in service, but all new URLs, such as in notifications, will use &lt;custom_domain&gt;.</td>
<td>Only one URL can be designated as the instance URL. The other URLs associated with your instance can be active, but only the instance URL can use notifications.</td>
</tr>
<tr>
<td>The Custom URL &lt;custom_domain&gt; is set to be immediately removed from the instance configuration and revert back to &lt;base.service-now.com&gt;. &lt;custom_domain&gt; 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. Accepting this confirmation initiates 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.url. 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 &lt;custom_domain&gt; does not point to &lt;base.service-now.com&gt;.</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 &lt;custom_domain&gt;.</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>

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, it has several key differences:

- The Normalization Data Services 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).
- For Helsinki, the Normalization Data Services plugin applies only to the manufacturer field for configuration items and assets.

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. This change occurs 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>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<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.

Sometimes a metric can be easily obtained from the data. For example, to find the number of incidents that were created today, a report will simply count the number of incidents in the
incident table with a Created date of today. Often, however, metrics need to 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 will be gathered, and instances of the metric will be calculated and stored. By an instance we mean a specific occurrence. For example, the "Assigned to Duration" metric measures the duration of time an incident is assigned to an individual. The metric is defined by creating a metric definition of type "Field value duration" and selecting the "Assigned to" field from the Incident table. A metric instance is then created for each incident assignment showing its duration. Reporting on the duration of incident assignments becomes easy.

Reporting on a metric is done using the database view that links the metric to the table on which it is defined.

**Create a metric**

Create a metric definition for a task table.

1. Navigate to **Metrics > Definitions**.
2. Click **New**.
3. Complete the Metric definition form then click **Submit**.

<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>
<tr>
<td>Table</td>
<td>Select the table that you want to collect metrics for. A metric can only apply to one table.</td>
</tr>
</tbody>
</table>

**Note:** The list shows only tables and database views that are in the same scope as the metric definition.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
<td>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.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<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 time from when the value of the specified field is set until it is changed. A Field value duration metric can optionally specify a script. The script can either return a duration value or set the answer variable to false to stop processing the metric. For example, the baseline incident metrics stop calculating duration when the Active field of an incident is set to false. The script can also carry out any other action such as closing the duration of other metrics defined on the same record. 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 using a script. The script has access to the current row in the table (for example an incident) and the metric definition. The script must perform metric calculations and insert data into the metric_instance table. The calculation does not have to result in a duration. It can calculate 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><em>(Optional)</em> 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 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.

```sql
// 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 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.
**Metric plugin**

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.

• Application server response: Time for the application server to process a request and render the resultant page.
• Network latency and throughput: Time for the network to pass your request to the server and the response back.
• Browser rendering and parsing: Time for your browser to render the HTML and parse/execute Javascript.
• Instance Cache: The amount of system resources available for processing.

**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 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.

![Browser response time details](image)

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:

```
ping -t <yourinstancename>.service-now.com
```

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 <yourinstancetype>.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   33 ms   33 ms  tbr2-cl1521.phmaz.ip.att.net [12.122.10.194]
6    32 ms   33 ms   33 ms  tbr2-cl1592.dlstx.ip.att.net [12.122.10.81]
7    31 ms   50 ms   31 ms  gar1-p370.dlrtx.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  gil-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 <yourinstancetype>.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**: apod0241-ia4.service-now.com:demoniighty/helsinki001
- **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

<table>
<thead>
<tr>
<th>Memory (MB)</th>
<th>613.0 of 1980.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>JVM Classes</td>
<td>27929.0 loaded, 1503.0 unloaded</td>
</tr>
<tr>
<td>Transactions</td>
<td>82905</td>
</tr>
<tr>
<td>Errors</td>
<td>218</td>
</tr>
<tr>
<td>GC.ConcurrentMarkSweep.Count</td>
<td>329 (2 per 5 minutes)</td>
</tr>
<tr>
<td>GC.ConcurrentMarkSweep.TotalTime</td>
<td>2222/86 (4 minutes)</td>
</tr>
<tr>
<td>GC.ConcurrentMarkSweep.AvgTime</td>
<td>0.88840435</td>
</tr>
<tr>
<td>GC.ParNew.Count</td>
<td>7425 (47 per 5 minutes)</td>
</tr>
<tr>
<td>GC.ParNew.TotalTime</td>
<td>1444/83 (2 minutes)</td>
</tr>
<tr>
<td>GC.ParNew.AvgTime</td>
<td>0.019453676</td>
</tr>
</tbody>
</table>

#### 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**: Not set
- **SMTP Status**: There is currently no active SMTP account configured, cannot send email

#### Database overview
- **URL**: jdbc:mysql://db01044-ia4.service-now.com:3441/a58b33df17b58a5
- **Name**: demoniighty/helsinki_1
- **Driver**: sh伽ービDB_2
- **Type**: 1.1
- **Version**: 5.6.10-log
**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:

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.glide.monitor.round_robin_database.

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](#)), ([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.

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.

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**

| Transactions | Any transaction type includes server-side and related client-side transactions. Metrics include **Total server load time**, which aggregates the total server-side time excluding semaphore and session wait times. It also aggregates relevant server transaction times that are found on the syslog_transaction table. Transaction types:
|              | • An HTTP Request transaction is identified by a URL, transaction type, processor, form/list action, URL query (filters), and related table name. |

© 2019 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.
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>Field</th>
<th>Description</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>
</tbody>
</table>

© 2019 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 | Description
--- | ---
Has | The hash value for this record.
Label | The mutex lock label.
Example URL | The URL for an individual mutex lock.
Event Execution Time / Event Count Trend graphs | The Mutex Execution Time Trend graphs show the total execution time of these mutex locks over the most recent 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
Administrators can use slow events logs to gain insight into how events are affecting platform performance.

### Field | Description
--- | ---
Event name | The name of the event for this record.
Queue | The event queue containing this event.
Execution count | The number of similar occurrences that are aggregated.
Average execution time (ms) | The average duration to execute one of these similar events.
Day moving average (ms) | An average of the moving average values of execution time, calculated over periods of one day.
Last sighting | The time and date the last occurrence was noted.
First sighting | The time and date the first occurrence was noted.
Hash | The hash value for this record.
Month moving average (ms) | An average of the moving average values of execution time, calculated over periods of one month.
Label | The event label.
Example URL | The URL for an individual event.
Example stack trace | An example stack trace for an individual event.
Total execution time | The sum of execution time for the aggregated occurrences.
Event Execution Time / Event Count Trend graphs | The 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. The Event Count Trend graphs show the event counts over the most recent period of two hours, one day, or one month.
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**

   ![Image of Slow Queries log]

   **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>
</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 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>
<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. For example, if a user navigates to the incident list, the URL is /incident_list.do sysparm_query=active=true.</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.

---

**Note:** The ISE supports MySQL databases only.

---

**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>ISE generated an index suggestion for the slow query.</td>
</tr>
<tr>
<td>Suggested</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—Unused</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>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>Index in progress</td>
<td>You scheduled the index for creation.</td>
</tr>
<tr>
<td>Creation Scheduled</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 ServiceNow Technical 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>Export</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>Ignore</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>
<tr>
<td>Schedule creation</td>
<td>Opens the Schedule Index Creation window for scheduling index creation.</td>
</tr>
</tbody>
</table>

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:
From the Application Navigator

Navigate to System Diagnostics > Index Suggestions > Index Suggestions > To review.

From the Performance homepage

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.

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 <code>Index suggestion states</code> 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>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</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 Index Suggestions &gt; Done 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.

   ![Location Description](Location Description)

<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, 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:

<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 has a number ( ), click the icon to open the Suggested Indexes window, and click View all suggested indexes.</td>
</tr>
</tbody>
</table>

   **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.

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.
Query Performance Test Results

<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 ServiceNow Technical 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.

---

### Schedule Index Drop

**Select Time**

- [ ] Drop now
- [x] Drop later

![2017-05-06 17:17:57](image)

- **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.
• **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 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.

![Welcome: James Capaldo](welcome.png) **Running: 26.1s**

**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.

![Welcome: James Capaldo](welcome.png) **Completed: 9.0s**

Transaction completed

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 <strong>System Properties &gt; UI Properties</strong></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 to the 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.</td>
</tr>
<tr>
<td></td>
<td>Type: Boolean</td>
</tr>
<tr>
<td></td>
<td>Default value: true</td>
</tr>
<tr>
<td></td>
<td>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 performance metrics.
The **System Overview** chart can be added to any homepage. For more information, see [Add existing reports to a homepage](#).

## 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.

The 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

You can also filter the data in each graph by using different measurements, such as maximum and minimum values, means, and medians.

The graph sets provide performance data for the following functional areas: Asynchronous Message Bus (AMB), Database, Discovery, MySQL Global Status, ServiceNow Servlet, and Slow Pattern. Some of these graphs are intended for use by ServiceNow Technical Support to troubleshoot performance issues or help you tune your system for maximum efficiency.

To open the Performance homepage, navigate to **Self-Service > Homepage** and in the homepage list, select **ServiceNow Performance**.

**Note:** An administrator or any user who can modify a homepage can also add performance metric graphs to a custom homepage. For more information, see [Add existing reports to a homepage](#) and [Customize your homepage content](#).

## Performance homepage features

The Performance homepage provides the following graph and display controls.
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, and 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  
<p>|        | - <strong>Compare with graph list</strong> - Graph overlay feature that lets you select a graph from a different data source and compare it to the current graph set. |
| 2      | <strong>Suggestion</strong> icon - Opens the Index Suggestion window, which provides links to index suggestions that have been created for slow queries. For details, see <a href="#">Review index suggestions for slow queries</a>. |</p>
<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
</table>
| 3      | Display controls:  
|        | • Information tooltip - Point to an area to see details about it.  
|        | • Documentation icon - 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. |
| 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 fullscreen 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 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 events displayed 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>

### ServiceNow servlet performance metrics

Each instance has a servlet, and you can monitor its performance using the servlet graph set on the Performance homepage.
To view servlet graphs on the Performance homepage, select ServiceNow Servlet in the Graph Set list, an instance in the Monitorable Items list, and a time period in the Timespan list.

For details on using the graph and display controls on the Performance homepage, see Performance metrics.
Graph Set: ServiceNow Servlet

Monitorable Items: demo

Timespan: 1 day

### System Overview
- Active Threads
  - Time span: 18:00 to 15:00
  - Metrics: CPU, Database, Business Rule, Network, Concurrency

### Transactions
- Transactions per Minute
  - Time span: 18:00 to 15:00
  - Metric: UI Transactions

### Response Time
- Response Time (ms)
  - Min, Average, Max
  - Time span: 18:00 to 15:00

### Sessions
- Active Sessions
  - Time span: 18:00 to 15:00
  - Metric: Count

### Session Wait Queue
- Waiting
  - Time span: 18:00 to 15:00
  - Metrics: Min, Average, Max

### Semaphore Use
- In Use
  - Time span: 18:00 to 15:00
  - Metric: Count
- **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 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 CPU.
- **Sessions**: Shows active sessions, including those sessions initiated by the MID Server and external integrations. A large number 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 ServiceNow Technical Support 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 ServiceNow Technical Support.
- **Scheduler**: Displays all scheduler activity for the selected instance, including Discovery 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.
- **Java Memory**: Records memory usage and indicates when the instance is running out of memory. The Java Memory graph is a useful problem indicator.
- **Java Garbage Collection Floor**: Shows the minimum memory floor and the memory currently consumed. Use this graph to identify high memory consumption. The higher the minimum
memory floor, the less memory is available for processing on the server. When less memory is available, excessive garbage collection (memory management) can occur, which can degrade performance. This graph can help identify low memory situations due to objects not picked up during garbage collection.

- **Garbage Collection Activity**: Shows the percent of time the server performs garbage collection. When the Java Virtual Machine (JVM) collects garbage, all processing stops until garbage collection is completed. High garbage collection times over a few percent can lead to service performance degradation.

- **Metaspace**: Shows the native memory used for storing the class metadata in Java SE Development Kit 8 (JDK 8). Metaspace replaces PermGen space in JDK 8.

- **Logs**: Shows the average number of logs created for the instance during the given timespan.

- **Errors**: Shows any severe errors printed to the localhost logs or syslog. 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.

### Database performance metrics

Database graphs, available to view on the 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.

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 are running on a single node, which is typical, the graphs show everything.

If you have the admin role, you can review performance metrics.

- To view database metrics on the Performance homepage, select Database in the **Graph Set** list, an instance in the **Monitorable Items** list, and a time period in the **Timespan** list.

- For details on using the graph and display controls on the Performance homepage, see **Performance metrics**.
- **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. ServiceNow Technical Support uses this information to monitor the progress of replicating a customer instance.

### Discovery performance metrics

Discovery metrics, available to view on the Performance homepage, measure the performance of the probes and sensors in your instance as they collect information about configuration items (CIs) in the network.

**Note**: Functionality described here requires the Discovery plugin.

Users with the admin role can review performance metrics.

- To view Discovery metrics on the Performance homepage, select Discovery in the **Graph Set** list, an instance in the **Monitorable Items** list, and a time period in the **Timespan** list.
- For details on using the graph and display controls on the Performance homepage, see [Performance metrics](#).

The available measurements to apply are **Count**, **Maximum**, **Mean**, **Median**, and **Minimum**. All times in these graphs are measured in milliseconds.
Discovery graphs
• **Discovery Probe Run Time**: Indicates elapsed time, in milliseconds, that probes take to run. Use this chart to check the performance of your MID Server. Slow run times can indicate a resource problem on the MID Server machine.

• **Discovery Sensor Queue Time**: Indicates how long a sensor task sits in the scheduler queue on the instance before it runs.

• **Discovery Sensor Run Time**: Measures how long a sensor task takes to run after it is started.

**MySQL Global Status performance metrics**

The MySQL Global Status graphs, available to view on the 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/instance.

Users with the admin role can review performance metrics.

• To view metrics for MySQL server status global variables on the Performance homepage, select MySQL Global Status in the **Graph Set** list, an instance in the **Monitorable Items** list, and a time period in the **Timespan** list.

• For details on using the graph and display controls on the Performance homepage, see **Performance metrics**.

**Note**: The MySQL Global Status graphs are intended for use by ServiceNow Technical Support to troubleshoot performance issues.
Slow pattern metrics

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 Performance homepage.

Users with the admin role can review performance metrics.

- To view slow pattern graphs on the Performance homepage, select Slow Pattern in the Graph Set list, an instance in the Monitorable Items list, and a time period in the Timespan list.
- For details on using the graph and display controls on the Performance homepage, see Performance metrics.

**Note:** 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.
Asynchronous Message Bus metrics

The Asynchronous Message Bus (AMB) graphs, available to view on the Performance homepage, monitor the transaction count and response times for transactions using asynchronous communication.

Users with the admin role can review performance metrics.

- To view AMB graphs on the Performance homepage, select AMB in the Graph Set list, an instance in the Monitorable Items list, and a time period in the Timespan list.

  **Note:** The AMB graphs are intended for use by ServiceNow Technical Support to troubleshoot performance issues.

- For details on using the graph and display controls on the Performance homepage, see Performance metrics.
AMB performance graphs

Table rotation

Table rotation preserves instance performance and averts risk associated with querying growing data sets by using 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.

Disk partition statistics

Disk partitions let you view the input and output statistics for partitions on the server that hosts your ServiceNow instance.

The available measurements are the read and write requests per minute and the number of bytes read and written per minute.
Disk partition performance metrics

You can display the statistics for each partition or the cumulative totals for all partitions. To view cumulative I/O for the entire disk, select the first item in the CI choice list. Select one of the individual partitions from the list to view the statistics for that partition alone.
Four of the disk partitions that appear in the list are generated as business services and are used to populate the performance graphs with data. If they are deleted, the instance automatically regenerates them. They appear in the list of business services.

Business services disk partitions

Linux statistics

The Linux Stats graph displays performance data for the server on which your instance is running. These graphs are used as a tool to locate and resolve issues with your instance.

- **CPU Usage**: The measurement of this graph indicates the percentage of the available CPUs that are running on this machine. This aggregated data indicates what portion of the machine's resources are being used at any given time. The most useful metric on this chart is the **IOWait** time measurement, which can indicate performance issues.

- **Load**: The load on the Linux machine indicates the average sum of the number of processes waiting. It includes those processes executing over increments of 1 minute, 5 minutes, and 15 minutes.
**CPU usage metrics:**

The following selections are available for CPU metrics.

- **Idle:** No threads are running. This statistic indicates the percentage of the machine's CPUs that are idle.
- **IOWait**: Indicates how long the CPU spends in a waiting state for disk or network I/O.
- **Nice**: View threads with a modified (lower) scheduling priority that configures them to be run when time permits.
- **System**: Displays the percentage of a single CPU that is being used to run system threads.
- **User**: Displays threads initiated by the application (the instance and the database).

**Apply table rotation**

You can apply table rotation by specifying the time parameter (duration) of the process and the number of tables (rotations) within.

Role required: admin

**Note:** Deploy this plugin in partnership with a ServiceNow representative.

1. Navigate to **System Definition** > **Table Rotations**.
2. Click **New**, or select the table rotation group to modify.
3. Set the table rotation fields.

<table>
<thead>
<tr>
<th>Table rotation group fields</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Duration</td>
</tr>
<tr>
<td>Initialized</td>
</tr>
<tr>
<td>Type</td>
</tr>
<tr>
<td>Rotations</td>
</tr>
<tr>
<td>Clean base rotation</td>
</tr>
</tbody>
</table>

4. Click **Submit** or **Update**.

**Note:** Deleting a rotation deletes the additional tables and all the data. Do not delete the rotation if the data is needed.

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. The group includes the original table plus a number of additional tables.
### Table Rotation Group - syslog

**Name**: syslog

**Duration**: Days 7

**Type**: Rotation

**Clean base rotation**: 2017-01-12 15:14:25

---

**Related Links**

### Synchronize Shards

---

**Table Rotation Schedule**

**Name**: syslog

<table>
<thead>
<tr>
<th>Offline</th>
<th>Table name</th>
<th>Valid from</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Log Entry [syslog0007]</td>
<td>2017-01-04 03:00</td>
</tr>
<tr>
<td></td>
<td>Log Entry [syslog0006]</td>
<td>2016-12-28 03:00</td>
</tr>
<tr>
<td></td>
<td>Log Entry [syslog0000]</td>
<td>2016-11-16 03:00</td>
</tr>
<tr>
<td></td>
<td>Log Entry [syslog0005]</td>
<td>2016-12-21 03:00</td>
</tr>
<tr>
<td></td>
<td>Log Entry [syslog0003]</td>
<td>2016-12-07 03:00</td>
</tr>
<tr>
<td></td>
<td>Log Entry [syslog0001]</td>
<td>2016-11-23 03:00</td>
</tr>
<tr>
<td></td>
<td>Log Entry [syslog0004]</td>
<td>2016-12-14 03:00</td>
</tr>
<tr>
<td></td>
<td>Log Entry [syslog]</td>
<td>1969-12-31 16:00</td>
</tr>
<tr>
<td></td>
<td>Log Entry [syslog0002]</td>
<td>2016-11-30 03:00</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.

### Available extension models

<table>
<thead>
<tr>
<th>Extension model</th>
<th>Flattens tables?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table per class</td>
<td>No</td>
</tr>
<tr>
<td>Table per hierarchy</td>
<td>Yes</td>
</tr>
<tr>
<td>Table per partition</td>
<td>Yes</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 /II/IID and the child class Computer might have a class path such as /II/IID/II.

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.

- **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]

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**
     - Navigate to **System Definition > Application Menus**.
     - 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
4. Click Submit.

**This ServiceNow instance**

Performance graph statistics are attached to the This ServiceNow instance business service. These statistics are the ones you can see on the Admin homepage when you add a Performance Graph Controls widget, and then add one or more performance graphs.

Do not delete this business service, or else the instance becomes unable to track its own performance.
This ServiceNow Instance
**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.

<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>
</tbody>
</table>
### Method Description

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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><code>getUser()</code></td>
<td>Returns the sys_id of the user.</td>
</tr>
<tr>
<td><code>getHomepage()</code></td>
<td>Returns the sys_id of the homepage.</td>
</tr>
<tr>
<td><code>getHomepageWidget()</code></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><code>glide.quota.manager.heartbeat</code></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><code>glide.quota.manager.minimum_transaction_time</code></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>
</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.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td>Default value: True</td>
<td>Location: Add to the (sys_properties) table</td>
</tr>
</tbody>
</table>
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>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</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>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Type</td>
<td>The type of transaction:</td>
</tr>
<tr>
<td></td>
<td>- <strong>List</strong>: Any list transaction, such as incident_list.do.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Form</strong>: All forms, UI pages, CMS pages, and so on.</td>
</tr>
<tr>
<td></td>
<td>- <strong>XMLHttp</strong>: Transactions that run through GlideAjax, where the URL is xmlhttp.do.</td>
</tr>
<tr>
<td></td>
<td>- <strong>SOAP</strong>: SOAP transactions.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Export</strong>: When a list is exported in a format such as XML or Excel.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Scheduler</strong>: When a scheduled job is performed.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Text Search</strong>: The text search transaction or any of its related operations.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Other</strong>: Any type that does not meet the qualities of another type.</td>
</tr>
</tbody>
</table>

**Note:** Match the transaction quota Type to the transaction type listed in the Quota Manager log entry for the transaction.

<table>
<thead>
<tr>
<th>User</th>
<th>The user performing the transaction.</th>
</tr>
</thead>
<tbody>
<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 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>Attributes</td>
<td>Miscellaneous attributes that are related to the transaction.</td>
</tr>
</tbody>
</table>

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=b55fbec4c0a800090088e83d7ff500de&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 url LIKE sys_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:


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.
Application quota property

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.quota.manager.cluster.update.seconds</td>
<td>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</td>
</tr>
</tbody>
</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>
<tr>
<td>Log only</td>
<td>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.</td>
</tr>
<tr>
<td>Maximum Events</td>
<td>The maximum number of events allowed during the update period.</td>
</tr>
<tr>
<td>Maximum Jobs</td>
<td>The maximum number of jobs allowed during the update period.</td>
</tr>
</tbody>
</table>
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>Condition</td>
<td>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.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the transaction quota.</td>
</tr>
</tbody>
</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 home.do.</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>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>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</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.  
- **XMLHttp**: Transactions that run through GlideAjax, where the URL is xmlhttp.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.  
| Note: Match the transaction quota **Type** to the transaction type listed in the Quota Manager log entry for the transaction. |
| 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 Extension.</td>
</tr>
</tbody>
</table>

4. Click Submit.

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 London

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 were 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>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>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>
</tbody>
</table>

Note: 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.
### ServiceNow London Now Platform Administration

#### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 or (disposition skipped manual merge and changed is true) or (disposition skipped and changed is true) or (disposition skipped(second pass) and changed is true), 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>Field</td>
<td>Input Value</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</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>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</td>
</tr>
<tr>
<td></td>
<td>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>
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.

---

**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 (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.

**Note:** By default, the list displays records with disposition of Skipped and resolution status of Not Reviewed.

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 <strong>Reviewed and Retained</strong>. The record moves from the Skipped Changes to Review to <strong>Skipped Changes Reviewed related list</strong>.</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Retain the customization by merging changes from the updated object.  | 1. Click **Resolve Conflicts** to navigate to the **Resolve Conflicts form**.  
2. Review the differences.  
3. 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. |

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 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>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>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Input Value</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td>Table</td>
<td>Table that contains the record.</td>
</tr>
<tr>
<td>File name</td>
<td></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>

**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.

**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>Field</td>
<td>Input Value</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</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 customs.</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 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>
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).

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.
<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>
<tr>
<td>Table</td>
<td>Table that contains the record.</td>
</tr>
<tr>
<td>File name</td>
<td>Current upgrade file name.</td>
</tr>
</tbody>
</table>
### File differences
Comparison of the file in the upgrade with the customized version.

### Changed by vendor
Indicates whether the file has been changed by the vendor since the last upgrade.

### 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.

### Field | Input Value
---|---
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.

Priority | Relative importance of the conflict that caused the skip based on the following criteria:
- 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

Resolution | - Reviewed
- Retained
- Reverted
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 HI knowledge base for known error articles
- Contact ServiceNow Technical 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 London, 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 London 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.
No Upgrade Detected

Current: glide-04-03-2017_1930.zip
Next upgrade check: 2017-04-04 17:00:00

Check Now

Upgrade Monitor

To check immediately for an available upgrade, click Check Now.

If one or both of the triggers for upgrading the system ('Upgrade' and 'Check Upgrade Script') 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 Fix Upgrade Jobs. This action reverts both upgrade triggers ('Upgrade' and 'Check Upgrade Script') to their base versions.

**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.
2. Monitor the progress of the upgrade.

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

#### 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>
</tbody>
</table>

© 2019 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>Screen element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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></td>
<td><strong>Note:</strong> 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.</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**

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

Screen elements

<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>
</tbody>
</table>

Review Skipped Updates | Click to reconcile conflicts that caused the system to skip some updates

### Node Upgrades

![Node Upgrades](image)

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 cmdbi attributes to cmdb.xml</td>
<td>21 Seconds</td>
<td>activate amb plugin.xml</td>
</tr>
<tr>
<td></td>
<td>rename cmdbi to cmdb</td>
<td></td>
<td>load the AMBI plugin early, to ensure feature upon first upgrade.</td>
</tr>
<tr>
<td>1 Minute</td>
<td>css fix index for identification.xml</td>
<td>20 Seconds</td>
<td>j_syslog_transaction_schema_change2_add.xml</td>
</tr>
<tr>
<td></td>
<td>Create database indices for out-of-the-box identification rules</td>
<td></td>
<td>Add the ACL field to syslog transaction without long after</td>
</tr>
<tr>
<td>31 Seconds</td>
<td>_metadata_conversion_6.xml</td>
<td>12 Seconds</td>
<td>activate live upgrade plugin.xml</td>
</tr>
<tr>
<td></td>
<td>Metadata conversion re-parenting</td>
<td></td>
<td>Used the Live Upgrade plugin early, to ensure feature upon first upgrade.</td>
</tr>
<tr>
<td>27 Seconds</td>
<td>fix_extended_web_server.xml</td>
<td>8 Seconds</td>
<td>activate_amb_msg_rolatation.xml</td>
</tr>
<tr>
<td></td>
<td>Move existing records in the web_server table to the new extended web-server tables based on the type of the web server</td>
<td></td>
<td>Activate task rotation on sys_amb_message</td>
</tr>
<tr>
<td>25 Seconds</td>
<td>fix promote database_application_fields.xml</td>
<td>7 Seconds</td>
<td>fix_related_list_calculated_name.xml</td>
</tr>
<tr>
<td></td>
<td>Promote Listener name to Database Instance, Edition and is clustered to Application</td>
<td></td>
<td>Fix sys-ui-related_list-calculated_name</td>
</tr>
</tbody>
</table>

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

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>Retain the customized record as is and do not update it.</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 <strong>Skipped Changes Reviewed related list</strong>.</td>
</tr>
</tbody>
</table>
| Retain the customization by merging changes from the updated object.   | 1. Click **Resolve Conflicts** to navigate to the **Resolve Conflicts form**.  
2. Review the differences.  
3. 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.  
  **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.                                      |

**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...
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**).
<table>
<thead>
<tr>
<th>Screen element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>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.

**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>
<tr>
<td>Resolution</td>
<td>How you elected to resolve this conflict:</td>
</tr>
<tr>
<td></td>
<td>- Not Reviewed</td>
</tr>
<tr>
<td></td>
<td>- Reviewed - reviewed but no action yet taken</td>
</tr>
<tr>
<td></td>
<td>- Reviewed and Merged - made changes to the record to reconcile the customized and upgraded versions</td>
</tr>
<tr>
<td></td>
<td>- Reviewed and Retained - left customizations in place without update from upgrade</td>
</tr>
<tr>
<td></td>
<td>- Reviewed and Reverted - 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 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>Type</td>
<td>The record type, for example Script include.</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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Base System</th>
<th>Customized</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Server side utility to support add relationship UI.</td>
<td>Server side utility to support add relationship UI.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>AddRelationshipAjax</td>
<td>AddRelationshipAjax</td>
</tr>
<tr>
<td><strong>Script</strong></td>
<td>var AddRelationshipAjax = Class.create({</td>
<td>var AddRelationshipAjax = Class.create({</td>
</tr>
<tr>
<td></td>
<td>AddRelationshipAjax.prototype = Object.extend(ObjectAbstractAjaxProcessor,</td>
<td>AddRelationshipAjax.prototype = Object.extend(ObjectAbstractAjaxProcessor,</td>
</tr>
<tr>
<td></td>
<td>});</td>
<td>});</td>
</tr>
<tr>
<td><strong>Prevention policy</strong></td>
<td>--None--</td>
<td>Revert only</td>
</tr>
<tr>
<td><strong>Replace on upgrade</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.
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 Update version history.

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.

Upgrade Transaction List

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of record processed during the last upgrade session.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Type</td>
<td>Type of record processed during the upgrade.</td>
</tr>
<tr>
<td><strong>Business rule</strong></td>
<td>Server-side script that runs when a record is displayed, inserted, updated, or deleted, or when a table is queried. See Business rules.</td>
</tr>
<tr>
<td><strong>Client script</strong></td>
<td>Client JavaScript run when client-based events occur. See Client scripts.</td>
</tr>
<tr>
<td><strong>Data policy</strong></td>
<td>Policies that enforce data consistency. See Data policy</td>
</tr>
<tr>
<td><strong>Script include</strong></td>
<td>Script includes that store JavaScript run on the server. See Script includes</td>
</tr>
<tr>
<td><strong>UI action</strong></td>
<td>Buttons, links, and context menu items on forms and lists. See UI actions</td>
</tr>
<tr>
<td><strong>UI macro</strong></td>
<td>Discrete scripted components added to the user interface. See UI Macros</td>
</tr>
<tr>
<td><strong>UI page</strong></td>
<td>Pages used to create and display forms, dialogs, lists, and other UI components. See UI pages</td>
</tr>
<tr>
<td><strong>UI policy</strong></td>
<td>Policies that change the behavior of information on a form and control custom process flows for tasks. See UI policies</td>
</tr>
</tbody>
</table>

**Note:** These are the only types of artifacts logged by the Upgrade Debugger.

| Last Modified | Date and time the record was last modified. |

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.
Express conversion to ServiceNow Enterprise

When a ServiceNow Express instance is converted to the ServiceNow Service Management enterprise platform, the instance is changed significantly.

The following topics help you understand what to expect during and after you convert from the ServiceNow Express platform to the ServiceNow Service Management enterprise platform. The topics provide advice and recommendations for advanced features and applications for you to consider.

It is recommended that you read the topics in the following order.

Express conversion to Enterprise overview

As you plan your upgrade from the ServiceNow Express platform to the ServiceNow Enterprise platform, become aware of the many features and resources that are available to you, both inside and outside of your instance.

Your upgraded instance will have significant new functionality that is part of the standard service management suite, including the following.

- **Graphical workflow**: Simplify complex service catalog requests with the highly configurable drag-and-drop Workflow Editor.
- **Scripting**: Extend your instance beyond standard configurations.
- **Content management**: Create a custom interface for the ServiceNow platform and ServiceNow applications.

In addition to the standard service management suite, there are additional applications and suites that your organization can purchase, for example, financial and human resources applications, and the operation management suite. The ServiceNow Express platform did not offer these solutions, and it is recommended that you explore the resources available to learn about extending your ServiceNow Enterprise instance.

Where you may have been using the Express support site forums for help, a larger Enterprise community site is now available.

There are many resources available on the community site and on YouTube, but the ServiceNow Demo Center is the best resource to quickly learn about Enterprise platform functionality. The Demo Center offers on-demand videos and live presentations where you can ask questions via chat.

[Click here to access the Demo Center](#). Enter email address you registered with ServiceNow as your username, and reset your password if you are attempting to access the Demo Center for the first time.

Recommended Demo Center videos for an organization that upgrades from the Express platform to the Enterprise platform include the following:

- Skinning the self service portals via Content Management
- Asset management life cycle
- Creating automation via Workflows

Working with support

After you become an Enterprise customer, you may receive XML files from support that are needed to fix issues. To import these XML files into your instance, navigate to any list view, right-click a column header, and select **Import XML**. Select the XML file you were provided and submit
it. The import takes place, although you see no confirmation or loading screen. You can import any XML file from any table list view. For example, if support provides XML files with report data, you can import the files from the Incidents list view, Import XML option.

**Express conversion to Enterprise process**

The conversion process includes an opportunity for you to review and test the ServiceNow Enterprise platform with a copy of your data before your production instance is converted.

**Conversion process**

The conversion process follows this timeline

1. A non-production instance is created from a cloned copy of your ServiceNow Express production instance. This non-production instance is for the full Enterprise Service Management platform.

2. You receive a letter indicating that you are entering a 15-day testing phase. The purpose is to verify that your ITIL and self-service portal users continue to experience the behavior they are familiar with.

3. After you verify with the non-production instance that the conversion completed and is acceptable, your designated Hi Administrator updates the change record advising ServiceNow support of your acceptance.

4. ServiceNow support schedules a full conversion of your Express production instance to ServiceNow Service Management. Your non-production instance is paired to it, and is available for you to configure new features, validate them, and roll them out to production.

**ESS and ITIL experience**

After an Express instance is converted to the Service Management platform, users with ESS and ITIL roles experience the look, feel, and behavior they are familiar with. They can access the same sets of applications and modules, lists and forms, and they experience the same underlying behavior. All functions that were accessible to ESS and ITIL users in the Express instance look and behave the same way for all users after the conversion.

For example:

- The incident form looks and works exactly the same way as it did in the Express instance. The same is true for the Problem, Change Request, and Configuration Item forms.

- Approvals are requested the same way as in the Express instance, and the approval process is the same.

- Survey responses are generated as in the Express instance.

**Administrator experience**

The Service Management platform is significantly different for administrators, who have access to all of its features. It is recommended that administrators attend the ServiceNow System Administrator training.
Express conversion to Enterprise considerations

Consider four core areas of functionality when planning your upgrade from the ServiceNow Express platform to the ServiceNow Enterprise platform. In these areas, Enterprise platform capabilities are more configurable, powerful, and flexible than in the Express platform.

Approval rule to workflow

As part of your migration from the Express platform to the Enterprise platform, reconsider your approval rules.

- In the Express platform, approval rules are applied to a record based on conditions when the record is saved. Approval rules run only when requested, and always occur first for catalog requests.
- In the Enterprise platform, approvals are an activity that is generally defined within the graphical workflow. This provides enhanced flexibility as you can define approval loops, re-approvals, and approvals that are nested at the beginning or end of a workflow. Reminder tasks can be defined to remind approvers that they need to take action.

Service level agreement (SLA) engine

The Express SLA engine is also record-based. In the Enterprise platform, the SLA engine has additional features, such as the ability to schedule jobs to auto-calculate time passed or time remaining metrics. In addition, workflow can be used to configure additional SLA complexity. You can activate the Service Level Management and SLA timeline plugins if they are not already active.

Security

The Express platform uses simple security for create, read, update, delete (CRUD) access through the dictionary. The Enterprise platform uses contextual security for more robust access control, referred to as access control lists (ACLs) or access control rules. During the conversion, your CRUD settings are converted to ACLs. The conversion does not change any of your security access.

The Enterprise platform offers additional benefits in the area of security. Security-based plugins are available and provide column level encryption, edge encryption, or encryption for data at rest. There are also a greater number of roles available in the Enterprise platform that provide more granular options for granting access to the appropriate users to take action. Going forward, you will manage security settings using ACLs. For more information, see Platform security.

Development Instance

On the Enterprise platform, you can utilize a development instance in addition to your production instance. The development instance gives you a place to test and validate new Enterprise configurations. As you make changes to the development instance, you can use update sets to track and push the configurations to your production instance.
Scripting and other configuration options

As an administrator of a ServiceNow Enterprise instance, you have more configuration options available than in an Express instance. For example, there are additional field types on forms and an extensive list of dictionary options for fields or tables.

Administrators have access to core ServiceNow platform features such as scripted business rules, client scripts, UI actions, UI pages, UI Macros, UI scripts, script includes, script actions, and so on. Administrators have access to all tables and dictionary entries, and can use scripting to accomplish any change in the instance. Examples of custom configurations include the following.

- You can use **UI actions** to define custom buttons.
- You can use **Client scripts** to define client-side scripts to run calculations or change fields dynamically before the form is saved.

Revisit your Express process as regards workflow and configuration in the context of how the Enterprise platform works. Determine ways to optimize your process based on Enterprise platform flexibility.

Enterprise plugins

The ServiceNow Enterprise platform offers enhanced functionality via plugins, and new plugins become available with each new release. When you upgrade, most plugins are not enabled on your converted Enterprise instance. This is slightly different from the plugins activated by default on a new Enterprise instance.

After the conversion, the administrator can navigate to **System Definition > Plugins** and review the list of plugins that are available and active. The administrator can also choose which capabilities to activate after the conversion. The **List of plugins (London)** lists the available plugins.

**List of plugins to consider activating after a conversion**

After the conversion is completed, review the plugins that are available and choose the capabilities to activate. The plugins listed below are not activated on an Express to Enterprise platform conversion. Learn about the functionality these plugins provide and determine which ones to activate.

For a description of plugins not linked below, review the description in the list of Jakarta plugins.

1. Assessments (com.snc.assessment_core)
2. Assessment Designer Common (com.glide.assessment_designer.common)
3. Asset Management (com.snc.asset_management)
4. Best Practice - Change Risk Calculator (com.snc.bestpractice.change_risk)
5. Best Practice - ITIL KPI Reports (com.snc.bestpractice.itil_kpi)
6. Best Practice - Task Survey Management (com.snc.bestpractice.task_survey)
7. Catalog Designer Common (com.glide.ui.ng.cc)
8. Change Management - CAB Workbench (com.snc.change_management.cab)
9. Change Management - Core (com.snc.change_management)
10. Change Management - Standard Change Catalog
    (com.snc.change_management.standard_change_catalog)
11. Change Management - State Model (com.snc.change_management.state_model)
12. Change Management Workflows (com.glideapp.workflow_change_management)
15. Contextual Security: Role Management V2 REST API (com.glide.role_management.inh_count.rest_api)
16. Contract Management (com.snc.contract_management)
17. Data lookup and record matching support for Service Catalog (com.glide.data_lookup.catalog)
18. Depreciation (com.snc.depreciation) installed with Asset Management
19. DHTMLX Scheduler Library (com.snc.dhtmlx.scheduler)
20. Expense Line (com.snc.expense_line)
21. Fixed Asset (com.snc.fixed_asset)
22. Guided Setup for Performance Analytics (com.snc.pa.guided_setup)
23. ITSM Guided Setup (com.snc.guided_setup_metadata.itsm)
24. My Assets (com.snc.asset_myassets)
25. Organization Management (com.snc.organization_management)
26. Problem Tasks (com.snc.problem_task)
27. Role Delegation (com.snc.role_delegation)
28. SCSS Bootstrap Theme (com.glide.ui.scss.bootstrap)
29. SCSS Content Provider (com.glide.ui.scss)
30. Service Creator (com.glide.service-creator)
31. Service Level Management (com.snc.sla)
32. Service Portal - Core (com.glide.service-portal)
34. Service Portal - Service Catalog (com.glide.service-portal.service-catalog)
35. Service Portal - Service Status (com.glide.service-portal.service-status)
36. Service Portal Configuration Pages (com.glide.service-portal.config)
37. Service Portal Designer (com.glide.service-portal.designer)
38. Service Portal for Enterprise Service Management (com.glide.service-portal.esm)
40. Service Portal Surveys (com.glide.service-portal.survey)
41. Software Asset Management Extensions (com.snc.sam)
42. Survey designer (com.glide.survey_designer)
43. User guide (com.glide.user_guide)

Additional ServiceNow features and applications

There are a large number of additional ServiceNow applications available for purchase after your conversion from the Express platform is complete.
The following list include some examples of these applications. Contact your sales representative for more information.

- Service Mapping
- Password Reset
- Automated Software or Configuration Deployment
- Automated External Script Execution
- Event Management
- Security and Vulnerability Management
- Cloud management
- Advanced reporting through Performance Analytics
- HR Service Management
- Project and Portfolio Management

Important features in the base system

Review the features listed below for an understanding of more ways to extend platform functionality.

- Update sets
- Service level agreements
- Workflow
- Project Management
- Agile development
- Import sets
- Transform maps
- LDAP
- Content Management System

Additional resources

A number of additional resources are available to learn more about the Enterprise platform. As mentioned, the Enterprise community is similar to Express forums, and it provides help and support to answer all of your questions. The community includes regional user conferences that are referred to as SNUGS (Service Now User Groups). Joining a SNUG is a great way to network and learn from other businesses that use the ServiceNow Enterprise platform.

Since the Enterprise platform comes with functionality to download and install update sets of external configurations, it is popular for users to share applications and configurations they have built via the Share portal.

Since the Enterprise platform has a large number of additional integration points, more pre-built content is available in the ServiceNow App Store. Certified partners are members of our large technology partner community, and through the App Store they offer popular applications and integrations to help you integrate with your 3rd party systems. The App Store is an excellent resource for acquiring additional functionality outside of ServiceNow applications and suites.
# Platform security

Security is built into all levels of the system. 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.

<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>• Requesting High Security Settings activation</td>
</tr>
<tr>
<td>Certificates</td>
<td>Your instance requires certificates to establish secure connections and validate signatures. Requires configuration before use</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>Web service security</td>
<td>Enforce security using basic authentication, mutual authentication, or WS-Security.</td>
<td>Active</td>
<td>• WS-Security</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>• Activate HTML sanitizer</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>• Configure 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</td>
<td>With domain separation you can separate data, processes, and administrative tasks into logically defined domains. Requires a separate subscription</td>
<td>Active</td>
<td>• Request domain separation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Domain separation setup and basic administration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Domain separation in Encryption Support</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Domain separation in Edge Encryption</td>
</tr>
</tbody>
</table>

© 2019 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>Feature</th>
<th>Description</th>
<th>Status</th>
<th>Top Tasks</th>
</tr>
</thead>
</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     | Use encryption contexts to allow or deny access to sensitive data based on user role. Requires configuration before use.                                                                                   | Active          | • Set up encryption contexts  
• Domain separation in Encryption Support  
• Encrypt or decrypt MID Server configuration file values |
| 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. | 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 |

### Instance Security Dashboard

If you do not have the Performance Analytics - Premium plugin installed and activated, use the Instance Security Dashboard to gain awareness of security controls, educate yourself about security resources, and take steps to configure and maintain application security standards within your instance and your applications.

If you do not already have the Performance Analytics - Premium plugin installed and activated, follow the procedure described in Get licensed Performance Analytics.

**Caution:** To ensure that your dashboard receives up-to-date security information with every upgrade, do not customize the Instance Security Dashboard. Test all changes to security settings before implementing them in a production environment.

Do one of the following to access the Instance Security Dashboard:

- Go to the System Administration home page, click the System Security tile, and then click Instance Security Dashboard.

**Note:** The Instance Security Dashboard, introduced in Jakarta, has been deprecated. The Instance Security Dashboard (PA) is an enhanced version of the Instance Security Dashboard that uses the Performance Analytics framework. The daily compliance score that appears in the Instance Security Dashboard (PA) differs from the score in the earlier...
now deprecated, Instance Security Dashboard. Each of these dashboards uses differing
calculation methods for their respective scores, with the Instance Security Dashboard (PA)
being the more reliable and accurate of the two.

On the Instance Security Dashboard, you can view the security compliance score for your
instance, learn more about recommended settings, and configure system properties from the
following categories:

**Input Validation**
Ensure the application is robust against all forms of input data, whether obtained from the user,
infrastucture, external entity, or database system.

**Access Controls**
Restrict user accounts to control resources on the instance.

**Authorization**
Apply authorization controls to the application.

**Authentication**
Configure credential and password requirements.

**Attachments**
Apply restrictions on all the attachments uploaded, downloaded, and managed on the
instance.

**Session Management**
Ensure that cookies and other session-related information are securely managed.

**Security Best Practices**
Apply best practices to increase the effectiveness of base system security measures on the
instance.

**Secure Communications**
Ensure that confidentiality and integrity are achieved through SSL certificates and associated
metadata.

**Security Whitelisting**
Enforce security on unauthorized content.

**Email Security**
Apply inbound email configurations for additional security over the default configurations.

**Logging/Errors**
Apply logging and auditing strategies so that suspicious activity is identified and acted upon in a
timely manner.

---

**Note:** Some settings require the security_admin role to configure. The Instance Security
Dashboard can only be modified in the global scope.

You can return to the Instance Security Dashboard at any time to adjust your settings and
manage the overall security health of your instance. The dashboard is automatically updated
based on the properties set on your instance. The Instance Security dashboard generates a
compliance score based on guidelines in the ServiceNow instance hardening customer security
document.
Instance Security Dashboard

Welcome to the Instance Security Dashboard. This dashboard provides awareness, education and tools to configure and maintain application security standards.

What Does My Compliance Score Mean?

Compliance percentage between 50% and 99% indicates moderate level of security controls within an instance. Please ensure mandatory and recommended controls are enabled as recommended in the ServiceNow Instance Hardening document.

Additionally, review any of the critical Security Alerts listed.

Security Alerts

Your event-based information is summarised here and automatically refreshes every minute.

- Failed login attempts Today: 12
  - Yesterday: 0
  - This Week: 12

- Admin logins Today: 18
  - Yesterday: 0
  - This Week: 18

- Security-admin logins Today: 18
  - Yesterday: 0
  - This Week: 18

- Admin users added Today: 17
  - Yesterday: 0
  - This Week: 17

Security Resources

- Hardening Document: The ServiceNow instance hardening document helps you understand and configure application security controls in the instance. View the instance hardening document.


- Jakarta Release: Security fixes: There have been a number of notable security fixes with Jakarta version of ServiceNow Platform. View the list of fixes.
**Note:** The Failed login attempts Today dashboard item displays only local logins. Failed SAML logins are not displayed.

**Instance Security Dashboard (PA)**

The Instance Security Dashboard (PA) shows the compliance effectiveness of your instance security controls, provides security event monitoring metrics, and lets you configure and maintain instance security settings.

Either the admin role or the security_dashboard_user role is necessary to access the Instance Security Dashboard (PA).

**Caution:** To ensure that your dashboard receives up-to-date security information with every upgrade, do not customize the Instance Security Dashboard (PA). Test all changes to security settings before implementing them in a production environment.

To access the Instance Security Dashboard (PA), navigate to System Security > Instance Security Dashboard (PA).

**Note:** The Instance Security Dashboard, introduced in Jakarta, has been deprecated. The Instance Security Dashboard (PA) is an enhanced version of the Instance Security Dashboard that uses the Performance Analytics framework. The daily compliance score that appears in the Instance Security Dashboard (PA) differs from the score in the earlier, now deprecated, Instance Security Dashboard. Each of these dashboards uses differing calculation methods for their respective scores, with the Instance Security Dashboard (PA) being the more reliable and accurate of the two.

On the Instance Security Dashboard (PA), you can view the security compliance score for your instance, learn more about recommended settings, and configure system properties.
ServiceNow Security Dashboard

- **Non-Compliant Items**: 15
- **Total Items**: 73

**Compliance Score - Daily**: 86%

- **Security Fixes**: There have been a number of notable security fixes with the London version of ServiceNow Platform.
- **Documentation**: Platform Security resource helps you better understand the Platform Security components and its associated feature sets.
- **Community**: Come join the conversations and learn from experts and peers at the ServiceNow Security Operations Community.
- **Hardening Document**: The instance hardening document helps you understand and configure Application Security controls on the instance.
Note: Some settings require the security_admin role to configure. The Instance Security Dashboard (PA) can only be modified in the global scope.

You can return to the Instance Security Dashboard (PA) at any time to adjust your settings and manage the overall security health of your instance. The Instance Security Dashboard (PA) generates a compliance score based on guidelines in the ServiceNow Instance Hardening guide.

**Overview tab**

Trends and graphs on the Overview tab are updated every night after the Performance Analytics job is executed at 2:00 a.m. local time.

Note: If any errors in execution of the Performance Analytics job occur because of the number of records, you can increase the max number of records per query using the `com.snc.pa.dc.max_row_count_indicator_source` and `com.snc.pa.dc.max_records` properties in the sys_properties table.

**Non-Compliant Items**

Number of security controls that are not compliant based on the ServiceNow security recommendations.

**Total Items**

Total number of security controls on the instance.

**Compliance Score - Daily**

Indicates how compliant your instance is with security controls. The score is modified daily based on the security configurations enabled or disabled on the instance. You can manage security configurations on the Hardening tab. Click the help icon at the upper right of the compliance score to see what your score means:

- 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.

Note: Based on the criticality of the controls, appropriate weights have been assigned to the configuration items represented in the compliance score.

**Security Fixes, Documentation, Community, and Hardening Document**

Links provide access to information on security fixes, other security-related user documentation, community-related articles, and the ServiceNow Instance Hardening document.

**Hardening tab**

Trends and graphs on the Hardening tab are updated every night after the Performance Analytics job is executed at 2:00 a.m. local time.

**Mandatory page**

Provides statistics on mandatory security configuration properties.
Recommended page
Provides statistics on recommended security configuration properties.

Optional page
Provides statistics on optional security configuration properties.

Mandatory, recommended, and optional security configuration properties are described in the ServiceNow Instance Hardening guide.

On all three of the Hardening pages,

- Click the Compliant tile to list compliant security controls on the Breakdowns tab and compliant records on the Records tab.
  - The Breakdowns tab lists control categories from the Instance Hardening guide. The column with the current day’s date lists the number of security controls in the category that are compliant as of this date. The Change column lists the number of security controls in the category that were changed or updated on the current date.
  - The Records tab lists the compliant mandatory, recommended, or optional security configurations and enables you to configure and use any of those configurations for greater compliance.

- Click the Non-Compliant tile to list non-compliant security controls on the Breakdowns tab and non-compliant records on the Records tab.
  - The Breakdowns tab lists control categories from the Instance Hardening guide. The column with the current day’s date lists the number of security controls in the category that are non-compliant as of this date. The Change column lists the number of security controls in the category that were changed or updated on the current date.
  - The Records tab lists the non-compliant mandatory, recommended, or optional security configurations and enables you to configure and use any of those configurations for greater compliance.

Events tab

Failed Logins, External Logins, Impersonations, Admin Users added, Security Elevations, and Admin Logins on the Events tab are updated automatically as events occur. Trends and graphs on the Events tab are updated every night after the Performance Analytics job is executed at 2:00 a.m. local time.

Security Events Today
Indicates the number of Failed Logins, External Logins, Impersonations, Admin Users added, Security Elevations, and Admin Logins in the instance during the current day.

Event Trends - Daily
Shows security event trends in the instance over time.

Number of Admin Roles
Indicates the number of users with various admin and high-privilege roles.

Metrics - Users vs Events
Shows metrics for different security events, indicates the number of users in admin and high-privileged roles, and breaks down security events by user.
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.

The three checks are evaluated independently in the order displayed above.

More Info

Requires role

<table>
<thead>
<tr>
<th>Role</th>
<th>itil</th>
</tr>
</thead>
</table>

Insert a new row...
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

Start

User requests access to an object

Find ACL rules matching object

Evaluate permissions of matching ACL rules

Matches Found

No Matches

Does the user have one of the required roles?

Yes

Is the Condition true?

No

Yes

Does the Script return true?

No

Yes

Grant user access to the object

Deny user access to the object

End
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>Operation</td>
<td>Results of failing an ACL rule on object</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>report_on</td>
<td>User cannot create a report on the ACL table. For more information, see <a href="#">Restrict report creation with an ACL rule</a>.</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 <a href="#">Restrict report creation with an ACL rule</a>.</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 Processes</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></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>Allows users to insert new records (rows) into a table.</td>
</tr>
<tr>
<td>read</td>
<td>Allows users to display records from a table.</td>
</tr>
<tr>
<td>write</td>
<td>Allows users to update records in a table.</td>
</tr>
<tr>
<td>delete</td>
<td>Allows users to remove records from a table or drop a table.</td>
</tr>
<tr>
<td>edit_task_relations</td>
<td>Allows users to extend the Task (task) table.</td>
</tr>
<tr>
<td>edit_ci_relations</td>
<td>Allows users to extend the Configuration Item (cmdb_ci) table.</td>
</tr>
<tr>
<td>save_as_template</td>
<td>Allows users to save a record as a template.</td>
</tr>
<tr>
<td>add_to_list</td>
<td>Allows users to view or personalize specific columns in the list mechanic.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Conditions and scripts are not supported.</td>
</tr>
<tr>
<td>list_edit</td>
<td>Allows users to update records (rows) from a list.</td>
</tr>
<tr>
<td>report_on</td>
<td>Allows users to report on tables. This operation is also valid for field ACL rules.</td>
</tr>
<tr>
<td>personalize_choices</td>
<td>Allows 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

Find first matching table ACL rule

No matches

Find first matching field ACL rule

No matches

Evaluate ACL permissions

Pass
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 operations:

<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.

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>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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 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>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 Script 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.</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.</td>
</tr>
</tbody>
</table>

**Note:** 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.

**Note:** Users with the admin role always pass this permissions check because the admin role automatically grants users all other roles.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
</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.
**Access Control Rules**

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.

The three checks are evaluated independently in the order displayed above.

**More Info**

**Requiring role**

| Role | Insert a new row... |
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 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. For more information about setting this property, see [Enable role auditing with Contextual Security: Role Management V2](#). For more information about the Audit Roles table, see [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 table (sys_user_has_role), 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.

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

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.

If not already active, Contextual Security: Role Management V2 activates these related plugins.

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.

1. Navigate to the System Properties (sys_properties) table.
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.
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><strong>Apply ACL script conditions to reference fields</strong></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><strong>Apply ACLs to AJAXGlideRecord (client-side Glide record)</strong></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><strong>Evaluate the admin override at the access level</strong></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><strong>Use ACL debugging and troubleshooting tools</strong></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: false</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>

**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>
</table>
| glide.security.admin.override.accessterm | Evaluates the admin override condition at the access term level.  
  - Type: true | false  
  - Default value: true for new instances, false for upgrades.  
  - Location: Add to the System Properties (sys_properties) 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 (号楼) 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>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;/&lt;Operation&gt;.</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><img src="#" alt="Green Checkmark" /></td>
<td>Indicates the table or field passed the criteria.</td>
</tr>
<tr>
<td><img src="#" alt="Red X Icon" /></td>
<td>Indicates the table or field did not pass.</td>
</tr>
<tr>
<td><img src="#" alt="Empty Gray Circle" /></td>
<td>Indicates the ACL evaluation did not need to be performed.</td>
</tr>
<tr>
<td><img src="#" alt="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>
<tr>
<td>You create a custom ACL rule that does not work properly.</td>
<td>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.</td>
</tr>
<tr>
<td>Your field ACL rule does not work properly.</td>
<td>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.</td>
</tr>
<tr>
<td>Your table ACL rule does not work properly.</td>
<td>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.</td>
</tr>
<tr>
<td>You can see a field in a list but not in form.</td>
<td>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.</td>
</tr>
<tr>
<td>Error or symptom</td>
<td>Solution</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>You receive an error message when trying to execute a processor or client-callable script include.</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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 is available with the Geneva release.

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>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>
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.
ACL execution plan window

<table>
<thead>
<tr>
<th>UI item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>The name of the ACL.</td>
</tr>
<tr>
<td>Tab name</td>
<td>If the ACL is create, read, write, or delete.</td>
</tr>
<tr>
<td>Row level</td>
<td>Row-level ACLs that run on this table.</td>
</tr>
<tr>
<td>Field level</td>
<td>Field-level ACLs that run only on this field (or column in the table).</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 administrator.

**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.

**General security settings properties**

Security settings provide several properties to control the level of security on your instance. There are two 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.
**Warning:** When implementing any of these security features, you must thoroughly test the features before deploying them in a production instance.

### General security settings

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Escaping and embedded script support</strong></td>
<td></td>
</tr>
<tr>
<td>glide.ui.security.allow_codetag</td>
<td>Supports embedding HTML code using the ( \text{code} ) tag.</td>
</tr>
<tr>
<td></td>
<td>• Default value: Yes</td>
</tr>
<tr>
<td>glide.ui.security.codetag.allow_script</td>
<td>Allows embedded HTML (using ( \text{code} ) tags) to contain Javascript tags.</td>
</tr>
<tr>
<td>glide.ui.escape_all_script</td>
<td>Forces all expressions within Jelly JavaScript ( &lt;\text{script type=&quot;text/javascript&quot;}&gt; ) tags to be escaped by default. Enforces escaping only if the type attribute in the ( &lt;\text{script}&gt; ) tag is empty, or if the value is text/javascript, text/ecmascript, application/javascript, application/ecmascript, or application/x-javascript.</td>
</tr>
<tr>
<td></td>
<td>• Default value:</td>
</tr>
<tr>
<td></td>
<td>• New/zbotted instances: Yes</td>
</tr>
<tr>
<td></td>
<td>• Upgraded instances: No</td>
</tr>
<tr>
<td><strong>Attachment limits and behavior</strong></td>
<td></td>
</tr>
<tr>
<td>com.glide.attachment.max_size</td>
<td>Sets the maximum file attachment size in megabytes.</td>
</tr>
<tr>
<td>glide.attachment.role</td>
<td>Lists the roles (comma-separated) that can create attachments.</td>
</tr>
<tr>
<td>glide.attachment.extensions</td>
<td>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.</td>
</tr>
<tr>
<td>glide.ui.attachment.force_download_all_mime_types</td>
<td>Forces download of all multipurpose internet mail extensions (MIME) type attachment files.</td>
</tr>
<tr>
<td></td>
<td>• Default value:</td>
</tr>
<tr>
<td></td>
<td>• New/zbotted instances: Yes</td>
</tr>
<tr>
<td></td>
<td>• Upgraded instances: No</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>glide.security.file.mime_type.validation</code></td>
<td>Enables (Yes) or disables (No) MIME type validation for file attachments. File extensions configured via <code>glide.attachment.extensions</code> are checked for MIME type during upload.</td>
</tr>
<tr>
<td><em>Default value:</em></td>
<td></td>
</tr>
<tr>
<td>• New/zbooted instances: Yes</td>
<td></td>
</tr>
<tr>
<td>• Upgraded instances: No</td>
<td></td>
</tr>
</tbody>
</table>

**Customer uploads**

These properties affect customer uploads only. They do not affect attachments.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>glide.ui.strict_customer_uploaded_static_content</code></td>
<td>When set 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 <code>glide.ui.strict_customer_uploaded_content_types</code></td>
</tr>
<tr>
<td><code>glide.ui.strict_customer_uploaded_content_types</code></td>
<td>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.</td>
</tr>
</tbody>
</table>

**Security Manager and options**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>glide.security.manager</code></td>
<td>Security Manager.</td>
</tr>
<tr>
<td><code>glide.sm.default_mode</code></td>
<td>Security manager default behavior in the absence of any ACLs on a table.</td>
</tr>
<tr>
<td><code>glide.security.strict.updates</code></td>
<td>Double-checks security on inbound transactions during form submission. Rights are always checked on form generation.</td>
</tr>
<tr>
<td><code>glide.security.strict.actions</code></td>
<td>Checks conditions on UI actions before execution. Normally, conditions are checked only during form rendering.</td>
</tr>
<tr>
<td><code>glide.security.granular.create</code></td>
<td>Enforces create (as opposed to write) rules on new records.</td>
</tr>
<tr>
<td><code>glide.security.explain.write.locks</code></td>
<td>Displays an explanation on locked form elements.</td>
</tr>
</tbody>
</table>

**Cookies**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>glide.ui.forgetme</code></td>
<td>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 system property <code>glide.ui.session_timeout</code>.</td>
</tr>
<tr>
<td><em>Default value:</em></td>
<td>Yes for new/zbooted instances</td>
</tr>
<tr>
<td><code>glide.ui.secure_cookies</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>glide.secure_cookie.debug</code></td>
<td>Secure session cookie debugging. Select to enable extensive debug logging of secure session cookie operations.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Security restrictions for execution of scripts originating from the client</strong></td>
<td></td>
</tr>
<tr>
<td>glide.script.use.sandbox</td>
<td>Run client-generated scripts (AJAXEvaluate and query conditions) inside a reduced-rights sandbox. If enabled, only those business rules and script includes with the <strong>Client callable</strong> check box selected are available, and certain back-end application programming interface (API) calls are disallowed.</td>
</tr>
<tr>
<td>glide.script.allow.ajaxevaluate</td>
<td>Enables the AJAXEvaluate processor.</td>
</tr>
<tr>
<td>glide.script.secure.ajaxgliderecord</td>
<td>Applies standard security access control lists (ACLs) to AJAXGlideRecord calls.</td>
</tr>
<tr>
<td></td>
<td>• Default value: Yes for new and upgraded instances. If Yes, cannot be changed to No.</td>
</tr>
<tr>
<td><strong>Miscellaneous</strong></td>
<td></td>
</tr>
<tr>
<td>com.glide.communications.trustmanager_trust_all</td>
<td>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 the system property to No.</td>
</tr>
<tr>
<td>glide.outbound.sslv3.disabled</td>
<td>When active, forces outbound connections from an instance to use the transport layer security (TLS) instead of the secure sockets layer (SSL).</td>
</tr>
</tbody>
</table>

Additional properties are available for High Security Settings.

**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.

External users must obtain, at minimum, the snc_external role. 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

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.
Explicit Roles plugin

The Explicit Roles plugin (com.glide.explicit_roles) provides the snc_external and snc_internal roles. When the plugin is activated:

- All users must have the snc_internal role to access internal resources, the snc_external role to access external resources, or both. Users without at least one of these roles cannot access either internal or external resources, 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, including 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.

This ensures that external users added before activating the Explicit Roles plugin do not have access to internal resource 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.

**Note:** The snc_internal and snc_external roles can be added or removed 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 is automatically assigned to external Customer Service Portal contacts. If the Customer Service Portal is not activated, this role must be manually granted to external users. Access to records is granted through ACLs.

**Content Management System** site access is also affected. CMS is set up with Sites (content_site), Pages (content_page), and other resources. Some of the sites may have the Login page configured.

- If CMS sites do not have the Login page configured, the public role is automatically added to the Read Roles field on Pages (content_page) if the field is empty.
- If CMS sites have the Login page configured, the snc_internal role is automatically added to the Read Roles field on Pages (content_page) if the field is empty.

**Note:** Do not move System update sets among instances with and without the Explicit Roles plugin enabled.

**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.

### 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.

### 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 only lasts 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](image-url)
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.
The security_admin role

**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 | 1. In the banner frame, click your user name.  
2. Select **Elevate Roles**. |
In the banner frame, click the lock icon (🔒) by your user name.

A dialog box appears.

![Elevate Roles dialog box]

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 that they want to elevate to.

**Role required:** security_admin

1. Log in as a user with the security_admin role.
2. Elevate roles to security_admin.
3. Navigate to `sys_properties.list`.
4. Set the `glide.security.strict_elevate_privilege` property to true.

When the user logs in, they are presented with a dialog window to select the role to which they can elevate.
High Security Settings

High Security Settings refer to several security options available in your instance.

There are two ways to set or change High Security Settings properties.

  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.

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.

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.

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](image)

Security Warning notification
## High Security Settings properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.ui.escape_text</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Default: Yes</td>
</tr>
<tr>
<td>glide.ui.escape_all_script</td>
<td>Forces all expressions within Jelly JavaScript <code>&lt;script type=&quot;text/javascript&quot;&gt;</code> tags to be escaped by default. Enforces escaping only if the type attribute in the <code>&lt;script&gt;</code> tag is empty, or if the value is <code>text/javascript</code>, <code>text/ecmascript</code>, <code>application/javascript</code>, <code>application/ecmascript</code>, or <code>application/x-javascript</code>.</td>
</tr>
<tr>
<td></td>
<td>Default: Yes in new instances</td>
</tr>
<tr>
<td></td>
<td>Default: Yes</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>glide.ui.secure_cookies</td>
<td>Enable secure session cookies: Enable additional cookie security. If Yes, strict session cookie validation is enforced.</td>
</tr>
<tr>
<td></td>
<td>Default: Yes</td>
</tr>
<tr>
<td>glide.security.password_reset.uri</td>
<td>For mobile Password Reset, URL that the user is taken to when the user taps the Forgot password? button.</td>
</tr>
<tr>
<td>glide.security.strict.updates</td>
<td>Double-check security on inbound transactions during form submission (rights are always checked on form generation).</td>
</tr>
<tr>
<td></td>
<td>Default: Yes</td>
</tr>
<tr>
<td>glide.security.strict.actions</td>
<td>Check conditions on UI actions before execution. Normally conditions are checked only during form rendering.</td>
</tr>
<tr>
<td></td>
<td>Default: Yes</td>
</tr>
<tr>
<td>glide.security.use_csrf_token</td>
<td>Enable usage of a secure token to identify and validate incoming requests. This token is used to prevent cross-site request forgery attacks.</td>
</tr>
<tr>
<td></td>
<td>Default: Yes</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>glide.ui.escape_html_list_field</td>
<td>Escape HTML for HTML fields in a list view.</td>
</tr>
<tr>
<td></td>
<td>Default: Yes</td>
</tr>
<tr>
<td>glide.html.escape_script</td>
<td>Escape JavaScript tags in HTML fields.</td>
</tr>
<tr>
<td></td>
<td>Default: Yes</td>
</tr>
<tr>
<td>glide.ui.forgetme</td>
<td>Remove the Remember me check box from the login page.</td>
</tr>
<tr>
<td></td>
<td>Default: Yes</td>
</tr>
<tr>
<td>glide.smtp.auth</td>
<td>Authenticate with the SMTP server by the user name and password properties.</td>
</tr>
<tr>
<td></td>
<td>Default: Yes</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This property is deprecated.</td>
</tr>
<tr>
<td>glide.script.use.sandbox</td>
<td>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 The script sandbox property.</td>
</tr>
<tr>
<td></td>
<td>Default: Yes</td>
</tr>
<tr>
<td>glide.soap.strict_security</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Default: Yes</td>
</tr>
<tr>
<td>glide.basicauth.required.wsdl</td>
<td>Require authorization for incoming WSDL requests.</td>
</tr>
<tr>
<td></td>
<td>Default: Yes</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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.</td>
</tr>
<tr>
<td>glide.basicauth.required.csv</td>
<td>Require basic authorization for incoming CSV requests.</td>
</tr>
<tr>
<td></td>
<td>Default: Yes</td>
</tr>
<tr>
<td>glide.basicauth.required.excel</td>
<td>Require basic authorization for incoming Excel requests.</td>
</tr>
<tr>
<td></td>
<td>Default: Yes</td>
</tr>
<tr>
<td>glide.basicauth.required.importprocessor</td>
<td>Require basic authorization for incoming import requests.</td>
</tr>
<tr>
<td></td>
<td>Default: Yes</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>glide.basicauth.required.pdf</td>
<td>Require basic authorization for incoming PDF requests. Default: Yes</td>
</tr>
<tr>
<td>glide.basicauth.required.rss</td>
<td>Require basic authorization for incoming RSS requests. Default: Yes</td>
</tr>
<tr>
<td>glide.basicauth.required.scriptedprocessor</td>
<td>Require basic authorization for incoming script requests. Default: Yes</td>
</tr>
<tr>
<td>glide.basicauth.required.soap</td>
<td>Require basic authorization for incoming SOAP requests. Default: Yes</td>
</tr>
<tr>
<td>glide.basicauth.required.unl</td>
<td>Require basic authorization for incoming unload requests. Default: Yes</td>
</tr>
<tr>
<td>glide.basicauth.required.xml</td>
<td>Require basic authorization for incoming XML requests. Default: Yes</td>
</tr>
<tr>
<td>glide.basicauth.required.xsd</td>
<td>Require basic authorization for incoming XSD requests. Default: Yes</td>
</tr>
<tr>
<td>glide.cms.catalog_uri_relative</td>
<td>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: Yes</td>
</tr>
<tr>
<td>glide.set_x_frame_options</td>
<td>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 &lt;frame&gt; or &lt;iframe&gt;. Sites can use this property to avoid clickjacking attacks by ensuring that their content is not embedded into other sites. <a href="https://developer.mozilla.org/en/the_x-frame-options_response_header">https://developer.mozilla.org/en/the_x-frame-options_response_header</a> Default: Yes</td>
</tr>
<tr>
<td>glide.ui.attachment.download_mime_types</td>
<td>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: text/html,image/svg,image/svg+xml</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>glide.security.groupby_acl_check</td>
<td>When this property is enabled, ACL checks for GroupBy operations are performed for the group names based on the actual data from the groups.</td>
</tr>
<tr>
<td>glide.security.diag_txns_acl</td>
<td>If set to Yes, only the admin user or user from allowed IP address can access stats.do, threads.do, and replication.do.</td>
</tr>
<tr>
<td>glide.ui.security.codetag.allow_script</td>
<td>Allow embedded HTML (using (code) tags) to contain JavaScript tags.</td>
</tr>
<tr>
<td>glide.script.allow.ajaxevaluate</td>
<td>Enable the AJAXEvaluate processor. The AJAXEvaluate API call allows the client to send and execute arbitrary scripts on the server.</td>
</tr>
<tr>
<td>glide.login autocomplete</td>
<td>Allow browsers to use auto-complete on password fields on login forms.</td>
</tr>
</tbody>
</table>

The following properties are defined in the sys_properties table, but are not visible on the High Security Settings page.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.glide.communications.httpclient.verify_hostname</td>
<td>Verify the hostname and certificate chain presented by remote SSL hosts. Protect against Man-In-The-Middle (MITM) attacks.</td>
<td>true</td>
</tr>
</tbody>
</table>

Note: This property overrides the com.glide.communications.trustmanager_trust_all property.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>glide.security.csrf_previous.allow</td>
<td>Allow usage of an expired secure token to identify and validate incoming requests. This token is used to prevent cross-site request forgery attacks.</td>
<td>false</td>
</tr>
<tr>
<td>glide.security.csrf_previous.time_limit</td>
<td>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.</td>
<td>86400 seconds or 1 day</td>
</tr>
<tr>
<td>glide.security.csrf.strict.validation.mode</td>
<td>Enforces strict validation on CSRF tokens so that users cannot resubmit a request if the CSRF token does not match.</td>
<td>false</td>
</tr>
</tbody>
</table>
The 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.

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><code>deleteMultiple()</code>, <code>deleteRecord()</code>, <code>insert()</code>, <code>update()</code>, <code>updateMultiple()</code></td>
</tr>
<tr>
<td>GlideSystem (gs)</td>
<td><code>addErrorMessage()</code>, <code>addInfoMessage()</code>, <code>addMessage()</code>, <code>eventQueue()</code>, <code>flushMessages()</code>, <code>getEscapedProperty()</code>, <code>getProperty()</code>, <code>setProperty()</code>, <code>setRedirect()</code>, <code>setReturn()</code>, <code>workflowFlush()</code></td>
</tr>
<tr>
<td>ScopedGlideRecord</td>
<td><code>deleteMultiple()</code>, <code>deleteRecord()</code>, <code>insert()</code>, <code>update()</code>, <code>updateMultiple()</code></td>
</tr>
<tr>
<td>ScopedGlideSystem (gs)</td>
<td><code>addErrorMessage()</code>, <code>addInfoMessage()</code>, <code>eventQueue()</code>, <code>executeNow()</code>, <code>getProperty()</code>, <code>getSessionToken()</code>, <code>setRedirect()</code></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; If enabled, only those business rules and script includes with the Client callable checkbox set to true are available and certain back-end API calls are disallowed.</td>
<td>Enabled (sandbox in use)</td>
</tr>
</tbody>
</table>

---

**Requesting High Security Settings activation**

The High Security Settings plugin is active by default on all new instances.

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.

If it is not active on your instance, you can request the plugin.

1. In the HI Service Portal, click Service Requests > Activate Plugin.
2. Fill out the form.

<table>
<thead>
<tr>
<th>Target Instance</th>
<th>Instance on which to activate the plugin.</th>
</tr>
</thead>
<tbody>
<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>Date and time must be at least 2 business days from the current time.</td>
</tr>
<tr>
<td>Reason/Comments</td>
<td>Provide any information that would be helpful for the ServiceNow personnel activating the plugin. For example, if you need the plugin activated at a specific time instead of during one of the default activation windows.</td>
</tr>
</tbody>
</table>

---

© 2019 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 Submit.

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:

1. Directs the user to a login page if not already logged in.
2. 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 a CMS Site:

When users log on to 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 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 CMS site form.

Logging Into a CMS Site to Access a Record:

When users log on to 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.

<table>
<thead>
<tr>
<th>Script action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNC User Lockout Check with Auto Unlock</td>
<td>- Uses the value of the <code>glide.user.max_unlock_attempts</code> property to set the limit for failed login attempts.&lt;br&gt;- Unlocks the user account after the time period that is specified for the <code>glide.user.unlock_timeout_in_mins</code> property. If no value is specified, then the system unlocks the user account after the default period of 15 minutes.</td>
</tr>
<tr>
<td>SNC User Lockout Check</td>
<td>Tracks the number of failed login attempts and locks the user account after a specified number of failed login attempts (default: 5).</td>
</tr>
<tr>
<td>SNC User Clear</td>
<td>Updates the user record after a successful login: Resets the number of failed login attempts and updates the date of the last login.</td>
</tr>
</tbody>
</table>

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: <code>$sp</code></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 does not work in UI16.

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.
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>
<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 setMaxInactiveInterval 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.

```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 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.

<table>
<thead>
<tr>
<th>Reset Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account is not locked</td>
</tr>
<tr>
<td>At least 8 characters</td>
</tr>
<tr>
<td>At least one uppercase and one lowercase letter</td>
</tr>
<tr>
<td>At least one number</td>
</tr>
<tr>
<td>New password</td>
</tr>
<tr>
<td>Retrieve password</td>
</tr>
</tbody>
</table>

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 /$pwd_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 Configure your Password Reset process for instructions on accessing this form and configuring the fields.

**Note:**

- This feature works for locally authenticated users who enter the username and password specified in their user record. Users logging in to the instance via an SSO solution or an LDAP integration cannot reset passwords with self-service Password Reset.
- The end user must enable and configure notification preferences. See Subscription-based notifications. Administrators can modify the email that is sent to the end user.
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.

Password Reset properties

<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></td>
<td></td>
</tr>
<tr>
<td>Email template for reminders to users who need to enroll for the password reset process</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>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>Property Label</td>
<td>Property Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>--------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Workflow expiration                               | password_reset.wf.timeout                  | Maximum wait time in milliseconds for the workflow to complete. The workflow is triggered during the password reset request when the user clicks **Submit**.  
- Type: integer  
- Default value: 90000  |
| Disable CAPTCHA validation functionality          | password_reset.captcha.ignore              | Enables or disables CAPTCHA functionality.  
- Type: true|false  
- Default value: false  |

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](#)

<table>
<thead>
<tr>
<th>Password Reset Request properties</th>
<th></th>
<th></th>
</tr>
</thead>
</table>
| Number of unsuccessful attempts allowed to reset/change password | password_reset.request.max_attempt         | 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**.  
- Type: integer  
- Default value: 3 (attempts)  |
| Number of minutes a user must wait to reset/change password after exceeding the maximum allowed unsuccessful attempts | password_reset.request.max_attempt_window | Time period that users are blocked or prevented from changing their passwords after trying the maximum number of times.  
- Type: integer  
- Default value: 1440 (minutes)  |
<table>
<thead>
<tr>
<th>Property Label</th>
<th>Property Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Number of minutes a user must wait to reset/change password after the last successful reset/change | password_reset.request.success_window                                          | Time period that a user must wait after successfully resetting the password to reset the password again.  
• Type: integer  
• Default value: 1440 (minutes)                                                                                                                                                                                                                                                   |
| Number of minutes a user must wait to start a reset request after the last successful unlock account | password_reset.request.unlock_window                                          | Time period that a user must wait after a successful unlock operation before starting a new request.  
• Type: integer  
• Default value: 1440 (minutes)                                                                                                                                                                                                                                                   |
| Number of minutes before a password reset request expires                      | password_reset.request.expiry                                                  | Time period during which a user must perform the Password Reset process.  
• Type: integer  
• Default value: 10 (minutes)                                                                                                                                                                                                                                                   |
|                                                                               |                                                                               | **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**                                |                                                                               |                                                                                                                                |
| Minimum number of characters in any answer                                    | password_reset.qa.ans_min_len                                                  | Minimum number of alphanumeric characters that the user must enter in the answer text box for any security question.  
Default value: 3 characters                                                                                                                                                                                                                                                         |
<table>
<thead>
<tr>
<th>Property Label</th>
<th>Property Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Number of security questions required during the password reset request | password_reset.qa.num_reset | 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.  
- Type: integer  
- Default value: 3 (questions)  
- Possible values: Integers that are less than the number specified for the **Number of security questions required during enrollment** property (the num_enroll parameter).  

**Note:** You can override this property setting for a Password Reset process by configuring the **num_reset** 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>
<tbody>
<tr>
<td>Number of security questions required during enrollment</td>
<td>password_reset.qa.num_enroll</td>
<td>Number of questions that a user must provide answers to while enrolling for the Password Reset process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type: integer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Default value: 5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Possible values: Integers that are greater than or equal to the number specified for the <strong>Number of security questions required during enrollment</strong> property (the num_reset parameter).</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> 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 <strong>Number of security questions required during enrollment</strong> property (the num_reset parameter).</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> You can override this property setting for a Password Reset process by configuring the <strong>num_enroll</strong> parameter. See <strong>Specify the number of required security questions</strong>.</td>
</tr>
</tbody>
</table>

Password Reset SMS Code properties
<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>
</table>
| Number of minutes before the SMS code expires                                | password_reset.sms.expiry         | Time, in minutes, until the SMS code sent to the user expires.  
  - Type: integer  
  - Default value: 5 (minutes)  
  
  **Note:** You can override this SMS code property by the `expiry` parameter in the SMS code verification. |

**Password Reset Monitoring and Reporting properties**

| Time interval, in minutes, for counting blocked users                         | password_reset.activity_monitor.incident_window | Time window to count the number of blocked users.  
  - Type: integer  
  - Default value: 60 (minutes) |
| Number of blocked users, in the defined time interval, that triggers a system log event | password_reset.activity_monitor.incident_threshold | Number of blocked (or locked) users, within the specified time window, that triggers a system log event.  
  - Type: integer  
  - Default value: 10 (blocked users) |

**Password Reset Style Sheet**

| Style sheet to apply to end-user pages during the password reset process.     | password_reset.stylesheet         | 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.  
  - Type: string  
  - Default value: `css_pwd_reset_default` |
<table>
<thead>
<tr>
<th>Property Label</th>
<th>Property Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Email template for reminder emails                 | password_reset.email_template_default             | 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:  
  · (Subject) Reminder: Enroll in the Password Reset program  
  · (Body) Click here to enroll for the password reset service.  
  
  **Note:** You must create an email template in the password_reset table to use it as a reminder.  
  · Type: string  
  · Default value: email_template_default                          |

**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.

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

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.

**IP Address Access Control**

By default the list is empty, meaning that there are no particular restrictions on access to your instance.

Role required: admin

Navigate to System Security > IP Address Access Control to see a list of your IP access controls. You may need to activate this module.

You can add these types of rules:

- **Allow:** any IP address in this range is allowed to connect to this instance.
- **Deny:** any IP address in this range is not allowed to connect to this instance unless it is listed in an allow rule.

**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 on the source instance.

**Example 1: Block a particular range**

An example of how to block a particular range.

Let’s say we want to block a particular range of IPs, say 64.236.16.0 – 64.236.16.255. Click ‘new’ to add a new rule. Then fill it in as follows. Range Start and Range End must be specific IP addresses as seen in the examples, without asterisks or CIDR blocks.

![Access Control](image)

Deny range

**Example 2: Block everyone except a particular range**

An example of how to block everyone except a particular range.

For example, you want to allow addresses between 64.236.16.0 and 64.236.16.255 to connect, but want to deny all other addresses. To do this, designate two rules, one to allow the designated range, and a second to deny addresses outside the range.

Click New and add a new rule. Then fill it in as follows.
Access Control

- Type: Allow
  - Range start: 64.236.16.0
  - Range end: 64.236.16.255
  - Submit

Allow range

Add the deny rule.

Access Control

- Type: Deny
  - Range start: 0.0.0.0
  - Range end: 255.255.255.255
  - Submit

Deny all

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:

```
```

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=V1QuWmmxSfBgfRS099X0cAjKo5Q=&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).

Nonce Installation Exit

© 2019 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.
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()) {
```
var userLoad = GlideUser.getUser(data);
if (userLoad == null)
    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_authentication";
}

} catch(e) {
    gs.log(e);
    return "failed_authentication";

}

// Encoded data didn't match received Encoded data

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();
ngnNew.u_nonce = sentNonce;
grNew.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.

**ServiceNow access control**

This SNC Access Control plugin (com.snc.snc_access_control) enables customers to control which ServiceNow employees may access their instance, and when.

When the plugin is first activated, ServiceNow employees cannot log into the customer’s instance. Any currently logged-in ServiceNow employees remain logged in. The customer creates records in the SNC Access Control table that grant access to specific SNC employees or all employees.

**Login security**

Security for authorized ServiceNow employee logins to customer instances employs encrypted tokens generated by a secure server. Only properly authenticated ServiceNow employees are granted access to a customer instances. 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 our customers to determine precisely which ServiceNow 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 our customer’s instances:

- **Security server:** The security server is a locked-down, Linux host that can only be accessed by ServiceNow security personnel. 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 the HI instance is compromised by an attacker.
- **Synthetic users:** The facility on customer instances that enables authorized ServiceNow 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 ServiceNow employee logon. This user exists only in memory and provides no ongoing privileges. ServiceNow can deauthorize any ServiceNow employee at any time, and if the SNC Access Control plugin is enabled, our customers can also deauthorize any ServiceNow employee at any time.
- **Tokens:** The security tokens are specific to a customer instance and a particular ServiceNow employee. In addition, the mechanism that generates the tokens only works with actual ServiceNow employee logins to HI, not impersonated users. Once a security token is generated, it may only be used by a specific ServiceNow employee to log into a particular customer instance.
- **Time limit:** Security tokens expire four hours after they are generated. This limits the utility of hijacked tokens, which can only be used during this short window.
- **Logging:** Logins by ServiceNow employees to customer instances are recorded as a login event, and every action taken by the logged-in ServiceNow employee is added to both the transaction log (in the database) and the instance log (on the file system, which is inaccessible to most ServiceNow employees). ServiceNow employee logins and actions are readily identifiable, since the user names all end in @snc (like frodo.baggins@snc). This provides our customers with easy-to-use, robust, and reliable security logging for non-employee access.
When a ServiceNow employee wants to log into a customer instance, the security processing flow is as follows:

1. A ServiceNow Support technician requests a login for the customer's instance through hi.service-now.com.
2. HI checks that the technician has the proper role authorizing access to customer 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 HI's 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 on the customer instance, 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 customers instance, using the special user name ending with @snc.
8. The customer's 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 customer 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 ServiceNow employees:

- Event logs: The event logs show all ServiceNow logins to a customer instance.
- Transaction logs: The transaction logs show all activity on the instance, including any efforts to delete logs.

Request ServiceNow access control

Customers must request the SNC Access Control plugin (com.snc.snc_access_control) from HI.

Role required: admin

1. In the HI Service Portal, click Service Requests > Activate Plugin.
2. Fill out the form.

<table>
<thead>
<tr>
<th>Target Instance</th>
<th>Instance on which to activate the plugin.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plugin Name</td>
<td>Name of the plugin to activate.</td>
</tr>
</tbody>
</table>

© 2019 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.
Specify the date and time you would like this plugin to be enabled. Date and time must be at least 2 business days from the current time. **Note:** Plugins are activated in two batches each business day in the Pacific time zone, once in the morning and once in the evening. If the plugin must be activated at a specific time, enter the request in the Reason/Comments.

<table>
<thead>
<tr>
<th>Reason/Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide any information that would be helpful for the ServiceNow personnel activating the plugin. For example, if you need the plugin activated at a specific time instead of during one of the default activation windows.</td>
</tr>
</tbody>
</table>

3. Click **Submit**.

**Configure ServiceNow access control**

Configure an access control record to specify one or more ServiceNow employees who have permission to log in your instance.

Role required: admin

1. Navigate to **System Security > SNC Access Control**.
2. Click **New**.
3. Fill in the form fields (see table).
4. Click **Submit**.

**SNC Access Control form fields**

<table>
<thead>
<tr>
<th>Form fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Names each ServiceNow employee who has permission to log in this instance. The names are expressed as firstname.lastname in lower case letters separated by a period (e.g., john.smith). Each name must have a corresponding user record in hi.servicenow.com. If more than one ServiceNow employee has permission to log in this instance, enter multiple names and separate them by commas. To allow all ServiceNow employees login rights to access the instance, enter an asterisk (<em>) in place of the name. For clarity, if you intend on restricting ServiceNow employee access to the instance, then the values in the Name field must not have an asterisk (</em>) anywhere in the field.</td>
</tr>
<tr>
<td>Reason</td>
<td>Human-readable field that describes why permission is being granted. This field is optional.</td>
</tr>
</tbody>
</table>
### Form fields

<table>
<thead>
<tr>
<th>Form fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start</td>
<td>Specifies the start date and time of the period during which the specified ServiceNow employees have login access. This field is mandatory.</td>
</tr>
<tr>
<td>End</td>
<td>Specifies the ending date and time of the period during which the specified ServiceNow employees have login access. This field is mandatory.</td>
</tr>
<tr>
<td>Active</td>
<td>Controls whether this permission record is active. The default is active.</td>
</tr>
</tbody>
</table>

### Audit logging

The following logging tracks logins and activity by ServiceNow employees.

**Event logs**

The event logs show all ServiceNow logins to a customer instance.

**Transaction logs**

The transaction logs show all activity on the instance, including any efforts to delete logs.

### 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><strong>Mutual authentication</strong></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 the Certificate Authority (CA) for a certificate. This ensures the instance accepts self-issued certificates. If you do not want to trust all certificates by default, set the following general security property to false: `com.glide.communications.trustmanager_trust_all`.

**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.

   ```bash
   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 Thwate 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
Note: 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 Valid from, Expires, Expires in days, Issuer, and Subject 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.

![Certificate](image)

**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 . getServiceResponse getSystemServiceResponse = 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:
  
  Demo_Incident. ServiceNowSoapClient client = new Test08WebService . Demo_Incident. ServiceNowSoapClient ( ) ;
  client . ClientCredentials . UserName . UserName = "admin" ;
  client . ClientCredentials . UserName . Password = "admin" ;
  
  Then in your app.config file look for the following and change "None" to "Basic":

  ```xml
  <transport clientCredentialType= "None" proxyCredentialType= "None" realm= "" />
  
  // When using VB .NET taking advantage of the Credentials object would look like the following:
  
  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
  DimgetResponse As New VB_Democm.incident.getResponse
  As New VB_Democm.incident.getResponse
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 only enables mutual authentication on outbound https connections. The instance does not support mutual authentication on inbound requests.

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.

```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
```

### 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.

![X.509 Certificate](https://example.com/uploaded/certificate.png) ![Required field](https://example.com/uploaded/required.png) ![Update](https://example.com/uploaded/update.png) ![Delete](https://example.com/uploaded/delete.png) ![Key store](https://example.com/uploaded/keystore.png) ![view](https://example.com/uploaded/view.png)

<table>
<thead>
<tr>
<th>Name:</th>
<th>Key store</th>
<th>Type:</th>
<th>Java Key Store</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active:</td>
<td>✔️</td>
<td>Key store password:</td>
<td>***************</td>
</tr>
<tr>
<td>Short description:</td>
<td>key store used for mutual authentication</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 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.

```plaintext
glide.httpclient.protocol.myhttps.class = "com.glide.certificates.DBKeyStoreSocketFactory"
glide.httpclient.protocol.myhttps.port = "4433"
```

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 Profiles](image)

**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)
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.
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 white 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 white list. Items can also be added to the black list, which overrides the white list, to remove HTML markup.

The following types of items can be added to white and black 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">Community</a>
```
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 white listed in the example above, this URL is not sanitized:

```html
<a title="Lotus" href="Notes://ABC/X575C90019DE33/ABC594DCB768EB4925653E0011C4C1/Z290B7E2D33964749257EEA003456FD">Lotus</a></p>
```

The Default White 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"]},
    colgroup:{attribute:["align","valign","char off","char","span","width"]},
```
Activate 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`. 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 black list, use the HTML_BLACKLIST class. To add items to the white list, use the HTML_WHITELIST class.

Use this format:

```
HTML_XXXXXLIST :{
  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"],
    attributeValuePattern:{src:".*jpeg"}},
  iframe:{},
}
```

It adds the following items to the white 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.
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.

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 just 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.

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 checked on the table dictionary and the table is not listed in the property glide.db.audit.ignore.delete.

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. This 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.
Any time an inactivity monitor touches a record. This 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. This is appropriate when you want to audit most, but not all, fields and is referred to as **blacklisting**. For more information, see *Exclude a field from being audited (blacklisting)*.
- You can enable auditing for the table but only for specified fields. This is appropriate when you want to audit only a small number of the table’s fields and is referred to as **whitelisting**. For information on how to include a field using whitelisting, see *Include a table field in auditing (whitelisting)*.

**Sys Audit and Audit Relationship Change tables**

The Now Platform tracks inserts changes to audited records in the Sys Audit (sys_audit) and Audit Relationship Change (sys_audit_relation) tables.

The Now Platform tracks audits tables for which you selected the Audit check box in the dictionary record. 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 display in 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: Displays the unique sys_id value of the changed record.</td>
</tr>
<tr>
<td></td>
<td>- Date and time fields: Displays the 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 table records tracks activity in tables that flagged for auditing. This activity includes journal field entries and history sets. The Audit Relationship Change (sys_audit_relation) table changes in the relationships between records in the sys_audit table, the source tables audit records originate from, and also tracks when a record may 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 sys_history_set, sys_history_line, and sys_journal tables.
- If you delete a field that is related to an audit table record, the deletion is recorded in the sys_audit_relation table. In other words, any time you change an audited record, the past history elements are first deleted, and a new relationship is created 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 whitelist auditing for a table. If you want to audit most – but exclude some – fields, Exclude a field from being audited (blacklisting).

### Enable whitelist 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 an audited table’s fields.

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 (blacklisting)

Prevent the system from tracking a subset of fields in an audited table by excluding those fields from the audit.

Role required: admin

To exclude a field in a table from being audited, you must have first enabled auditing for that table.

Blacklist a set of fields when you want to audit most of an audited table’s fields. If you need to audit only a few fields, follow the whitelisting 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 (whitelisting)**

Track a subset of fields in an audited table by whitelisting those fields.

Role required: admin

To whitelist fields in a table, you must have first enabled auditing for that table and enabled whitelist auditing for that table.

Whitelist a set of fields 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 blacklisting 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 whitelist.
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 generates history set records when a user requests to view an audited record's history.

Each record's History Set will be generated when the record is inserted, if the record is on an audited table. A user must view a record for the system to create or update a history set for that 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.

List View Record Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Input Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>A Document ID for the record whose history is being recorded.</td>
</tr>
<tr>
<td>Table</td>
<td>The audited table for the record whose history is being recorded.</td>
</tr>
<tr>
<td>Load Time</td>
<td>The amount of time it took to generate the history set.</td>
</tr>
</tbody>
</table>

Audit History Record Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Input Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>The label of the field which was changed.</td>
</tr>
<tr>
<td>Old</td>
<td>The value before the change.</td>
</tr>
<tr>
<td>New</td>
<td>The 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>The number of times this field has been changed. A value of -1 indicates when the record was created or deleted.</td>
</tr>
<tr>
<td>Update Time</td>
<td>The date and time of the change</td>
</tr>
<tr>
<td>User Name</td>
<td>The name of the user who created the change.</td>
</tr>
</tbody>
</table>
History Sets in a Calendar View

Once History Sets are active, the context menu choice History will populate 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 the way the information is stored is different.

The History view includes a calendar view, but does not use the normal list interface to filter and interact with the history records. This 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.

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 and 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.

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.

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. This means 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.
View History List

Click on a row item to view additional details about the change.
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.
### Incident History Detail

<table>
<thead>
<tr>
<th>Details for INC0000039</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Created</strong></td>
</tr>
<tr>
<td><strong>Last updated</strong></td>
</tr>
<tr>
<td><strong>Update count</strong></td>
</tr>
</tbody>
</table>

- 2012-04-05 17:42:29 Created by System Administrator (70 Days 19 Hours 34 Minutes)
- 2012-06-15 12:56:25 Updated by ITIL User (20 Minutes)

Highlight changes to field: [Assigned to]

<table>
<thead>
<tr>
<th>Week</th>
<th>Mon</th>
<th>Tue</th>
<th>Wed</th>
<th>Thu</th>
<th>Fri</th>
<th>Sat</th>
<th>Sun</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>28</td>
<td>29</td>
<td>30</td>
<td>31</td>
<td>June 1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>23</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>24</td>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15 Updated by ITIL User at 12:56:25</td>
<td>16</td>
<td>17</td>
</tr>
<tr>
<td>25</td>
<td>18</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>25</td>
<td>26</td>
<td>27</td>
<td>28</td>
<td>29</td>
<td>30</td>
<td>July 1</td>
</tr>
</tbody>
</table>

- **Field**
  - Assigned to: Bud Richman
  - Company: ACME
  - Incident state: Now Active
  - State: Now Active
  - Domain: global TOP/ACME
If you hover over the icon within an entry, a pop-up displays all the value changes. This is the same information that is displayed in the top part of the form.
### Incident History Detail

**Details for INC0000039**

<table>
<thead>
<tr>
<th>Created</th>
<th>2012-04-05 17:42:29 by admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last updated</td>
<td>2012-06-15 12:56:25 by itil</td>
</tr>
<tr>
<td>Update count</td>
<td>3 (1 audited)</td>
</tr>
</tbody>
</table>

#### 2012-04-05 17:42:29 Created by System Administrator (70 Days 1)

#### 2012-06-15 12:56:25 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 |
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 |

#### April 2012

<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></td>
<td>26</td>
<td>27</td>
<td>28</td>
</tr>
<tr>
<td>14</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>9</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>16</td>
<td>17</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>19</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>23</td>
<td>24</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>26</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>30</td>
<td>May 1</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td></td>
</tr>
</tbody>
</table>
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 change validation script](#).

---

© 2019 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.
**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 CIs represented by each bubble. Each snapshot displays the changes to the CIs 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 ( 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]).

Domain separation

Domain separation allows you to separate data, processes, and administrative tasks into logical groupings called domains. You can then control several aspects of this separation, including which users can see and access data.

**Explore**
- Upgrade to London
- Understanding domain separation
- Domain separation recommended practices for service providers

**Set up**
- Request domain separation
- Access the Domain Configuration console
- Create a domain

**Administer**
- Validate domain hierarchy
- View a list of tables using domain separation
- Delegated administration
Troubleshoot and get help

- Application support for domain separation
- Ask or answer questions in the forum
- Enable verbose domain logging and debug messages
- Search the HI Knowledge Base for known error articles
- Contact ServiceNow Technical Support

Learn

- Developer portal: Domain Separation
- Domain Separation Basics (Learning Portal login required)
- Domain Separation Configuration (Learning Portal login required)
- Domain Separation Troubleshooting (Learning Portal login required)

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. ServiceNow Technical 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 Black/Whitelist 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.

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

Visibility domains is 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 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 the user is granted access to a visibility domain, they always see data in that domain and its children.

Note: Using visibility domains excessively is not recommended. Although visibility is one method to allow users to access records, it is recommended that you 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 only grant visibility 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.

Contains domain example

A user has access to domain A (the user’s home domain) and is granted visibility to domains B and C. The user selects domain A in the domain picker. In this case, the user has access to domains A, B, and C. If the user changes the domain picker to domain B, B and C are visible. C is still visible because the user still has visibility to it. A is not visible, because it is not selected in the domain picker and it is not a visibility 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 Goodliffe cannot access Bow Ruggeri's incidents because of data separation.

Sample set of domain-separated incident records

Bow Ruggeri's incident list
You can add the database domain as a visibility domain to Bow Ruggeri’s user record. Then Bow Ruggeri can access Don Goodliffe’s incidents, since he now has visibility to the database domain. If you remove the visibility domain, then Bow Ruggeri can no longer access incidents in the database domain.

Inherit 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.

For example, as a member of the Database group, Don Goodliffe also automatically gains the Database domain as a visibility domain. Group membership grants visibility to any matching domain name.
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 MSP 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 MSP domain or collapse the domain scope to only show 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 managed 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 MSP 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>
<tbody>
<tr>
<td>The user has access to the domain of the current record referenced in a field.</td>
<td>The user can:</td>
</tr>
<tr>
<td></td>
<td>• See reference field display value. For example, sees the user name in the <strong>Assigned to</strong> field.</td>
</tr>
<tr>
<td></td>
<td>• See the related record from reference icon. For example, sees the user record for the user in the <strong>Assigned to</strong> field.</td>
</tr>
<tr>
<td></td>
<td>• Select values from any visible domain. For example, can select users from either the MSP and ACME domains.</td>
</tr>
<tr>
<td>The user does not have access to the domain of the current record referenced in a field.</td>
<td>The user can:</td>
</tr>
<tr>
<td></td>
<td>• See the reference field display value. For example, sees the user name in the <strong>Assigned to</strong> field.</td>
</tr>
<tr>
<td></td>
<td>• Only select values from the record’s domain. For example, can only select user’s from the ACME domain.</td>
</tr>
</tbody>
</table>
Domains and associated companies

Domain separation allows you to 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 have the ability to change their own user records and therefore can change domains. Managed 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.
Domain query methods

A domain query method allows the instance to efficiently query large numbers of domains.

**Note:** Domain paths are used for all customers on Helsinki and later. Domain numbering is no longer used. ServiceNow Technical Support can assist in the upgrade.

Part of Domain Support 2.0 is a new query engine designed to perform and scale to tens of thousands of domains. Prior methods, including domain numbering, have had limitations that domain paths resolves. While you have the flexibility to continue using your existing query method, we highly recommend that you switch to domain paths through the new Domain Configuration screen at your earliest convenience.

A domain path is a series of three-character codes separated by a slash (/) delimiter that uniquely identifies a domain. Each digit in the three-character code consists of one of the following 60 possible characters:

```
!#$&()*+,-.0123456789:<@ABCDEFGHIJKLMNOPQRSTUVWXYZ\[]^`{|~
```

The three-character codes that make up a path are not unique across a domain tree. Rather, the entire path string itself is unique. For example:
An example domain tree

Domain tree example

<table>
<thead>
<tr>
<th>Domain name</th>
<th>Parent domain</th>
<th>Domain path</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNC</td>
<td>None</td>
<td>!!!/</td>
</tr>
<tr>
<td>SNC/US</td>
<td>SNC</td>
<td>!!!/!!!/</td>
</tr>
<tr>
<td>SNC/EU</td>
<td>SNC</td>
<td>!!!/!!#/</td>
</tr>
<tr>
<td>SND/RU</td>
<td>SNC</td>
<td>!!!/!!$/</td>
</tr>
<tr>
<td>SNC/US/NY</td>
<td>SNC/US</td>
<td>!!!/!!!/!!#/</td>
</tr>
<tr>
<td>SNC/US/CA</td>
<td>SNC/US</td>
<td>!!!/!!!/!!$/</td>
</tr>
<tr>
<td>SNC/EU/DE</td>
<td>SNC/EU</td>
<td>!!!/!!#/!!!/</td>
</tr>
<tr>
<td>SNC/EU/FR</td>
<td>SNC/EU</td>
<td>!!!/!!#/!!!#/</td>
</tr>
</tbody>
</table>

**Note:** With three-character codes delimited by a single character in a path string of 255 total characters, each node of the domain tree supports up to 216,000 child domains, and the maximum depth of the tree is 63 levels.

Application support for domain separation

Not all ServiceNow applications support domain separation in the base system. Some supported applications include limitations on the data and administrative settings that can be domain separated.

Domain Separation support levels

Not all ServiceNow applications support domain separation. The applications that do may support the separation of data only, have advanced business logic separation, or support tenant level administration of the application. ServiceNow applications are defined with the following
incremental support levels. These definitions delineate the domain separation support level system, which operates from the perspective of actual use cases and personas.

**Data only**

Enables the separation of tenant data only in an application. It is not domain separated in the truest sense, because logic to route data to domains in the application is absent. All data created is placed in the current domain of the session creating the data.

**Level 1 — Tenant data management**

Level 1 support targets tenant domain Requester use cases in an application. The application has been designed to support Requester activities within tenant domains. Logic is in place to route data to tenant domains, based on applicable use cases. For example, a chat response of a parent to a child is placed in the domain of the child.

**Level 2 — Tenant process management**

Level 2 support targets tenant domain Fulfiller use cases in an application. A Fulfiller can use an application that supports Level 2 domain separation within the tenant domains. Business logic is domain separated, enabling tenants to act under separate processes as configured by an administrator. For example, comments are mandatory on close of a record for one tenant, but not another.

An application with Level 2 domain support includes Level 1 (Requester) support.

**Level 3 — Tenant self-managed configuration**

Level 3 support targets tenant domain no-code administrator use cases in an application. Applications with Level 3 domain separation support have been designed with prescriptive domain-separated configuration capabilities administered by a tenant domain administrator. For example, making the impact/urgency/priority matrix configurable by tenants to drive how priority is set within their domain.

An application with Level 3 domain support includes Level 1 (Requester) and Level 2 (Fulfiller) support.

<table>
<thead>
<tr>
<th>Supported feature</th>
<th>Data only</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported tenant domain user role.</td>
<td>Data only</td>
<td>Requester</td>
<td>Fulfiller</td>
<td>Administrator</td>
</tr>
<tr>
<td>Data can be domain separated.</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Domain column is present for base system application tables.</td>
<td>✔️</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>
<td>✔️</td>
</tr>
<tr>
<td>Tenant domains can manage their own application data.</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Application properties are domain aware when needed.</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Supported feature</td>
<td>Data only</td>
<td>Level 1</td>
<td>Level 2</td>
<td>Level 3</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------</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>
<td></td>
</tr>
<tr>
<td>Business logic and processes can be administered by tenant domain.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Application support for domain separation**

<table>
<thead>
<tr>
<th>Product Suite</th>
<th>Application</th>
<th>Support level</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Management</td>
<td>Agile Development</td>
<td>Data only</td>
<td>Product models not domain separated. System properties cannot be domain separated.</td>
</tr>
<tr>
<td></td>
<td>Application Portfolio Management</td>
<td>Data only</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cost Management</td>
<td>No support</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Financial Management</td>
<td>No support</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Project Portfolio Management</td>
<td>Data only</td>
<td>Architectural support only. Certain properties cannot be domain separated.</td>
</tr>
<tr>
<td></td>
<td>Release Management</td>
<td>No support</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Scaled Agile Framework (SAFe)</td>
<td>Data only</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Test Management</td>
<td>Data only</td>
<td></td>
</tr>
<tr>
<td>Custom Business Applications</td>
<td>Delegated Development</td>
<td>Data only</td>
<td>Application Administration must be enabled.</td>
</tr>
<tr>
<td></td>
<td>Script debugger</td>
<td>Level 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ODBC Driver</td>
<td>Data only</td>
<td>The ODBC user domain restricts access to data.</td>
</tr>
<tr>
<td></td>
<td>Web Services</td>
<td>Data only</td>
<td>Additional support possible, but depends on use case.</td>
</tr>
<tr>
<td>Customer Service Management</td>
<td>Communities</td>
<td>Data only</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Customer Service Management</td>
<td>Level 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Field Service Management</td>
<td>Level 1</td>
<td></td>
</tr>
<tr>
<td>Governance, Risk, and Compliance</td>
<td>Governance, Risk, and Compliance (GRC)</td>
<td>Level 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Vendor Risk Management</td>
<td>Data only</td>
<td></td>
</tr>
<tr>
<td>Product Suite</td>
<td>Application</td>
<td>Support level</td>
<td>Notes</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------</td>
<td>---------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>HR Service Delivery</td>
<td>HR Service Delivery</td>
<td>Data only</td>
<td></td>
</tr>
<tr>
<td>IT Operations</td>
<td>Cloud Management</td>
<td>No support</td>
<td></td>
</tr>
<tr>
<td>Management IT</td>
<td>Discovery</td>
<td>Level 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Event Management</td>
<td>Level 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Operational Intelligence</td>
<td>Level 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Service Mapping</td>
<td>Level 1</td>
<td></td>
</tr>
<tr>
<td>IT Service</td>
<td>Asset Management</td>
<td>Data only</td>
<td>License calculations supported in global scope only.</td>
</tr>
<tr>
<td>Management</td>
<td>Benchmarks</td>
<td>No support</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Change Management</td>
<td>Level 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Continual Improvement Management</td>
<td>Level 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contract Management</td>
<td>Data only</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Expense Line</td>
<td>Data only</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Incident Communications Management</td>
<td>Level 2</td>
<td>Can be separated through customization.</td>
</tr>
<tr>
<td></td>
<td>Incident Management</td>
<td>Level 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>On-Call Scheduling</td>
<td>Level 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Problem Management</td>
<td>Level 2</td>
<td>Task-outage relationship includes architectural support only.</td>
</tr>
<tr>
<td></td>
<td>Procurement</td>
<td>Data only</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Product Catalog</td>
<td>No support</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Request Management</td>
<td>Level 2</td>
<td>System properties cannot be domain separated.</td>
</tr>
<tr>
<td></td>
<td>Service Catalog</td>
<td>No support</td>
<td>For fulfillers, records created are domain separated based on table configuration. For requesters, user criteria can be used to achieve domain separation.</td>
</tr>
<tr>
<td></td>
<td>Service Desk Call</td>
<td>Level 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Service Level Management</td>
<td>Level 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Service Portfolio Management</td>
<td>Data only</td>
<td>Architectural support only.</td>
</tr>
<tr>
<td></td>
<td>Walk-up Experience</td>
<td>Level 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Vendor Performance</td>
<td>No support</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Agent Intelligence</td>
<td>Level 2</td>
<td></td>
</tr>
<tr>
<td>Now Platform</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Product Suite</td>
<td>Application</td>
<td>Support level</td>
<td>Notes</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------</td>
<td>---------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Assessments</td>
<td>Automated Test Framework</td>
<td>Data only</td>
<td>Because application tables are not domain separated, data is not visible in child domains.</td>
</tr>
<tr>
<td></td>
<td>Connect Support and Chat</td>
<td>Level 1</td>
<td>Connect Chat supported within each domain only. Connect Support dashboard and queues do not support domain separation.</td>
</tr>
<tr>
<td>Contextual Search</td>
<td></td>
<td>Level 2</td>
<td></td>
</tr>
<tr>
<td>Configuration Management (CMDB)</td>
<td></td>
<td>Level 2</td>
<td>CMDB CIs are domain separated.</td>
</tr>
<tr>
<td>Content Management System</td>
<td></td>
<td>Data only</td>
<td>Can be separated with customization.</td>
</tr>
<tr>
<td>Credentials and Connections</td>
<td></td>
<td>Level 1</td>
<td></td>
</tr>
<tr>
<td>Data Certification</td>
<td></td>
<td>Data only</td>
<td></td>
</tr>
<tr>
<td>Data Management</td>
<td></td>
<td>No support</td>
<td></td>
</tr>
<tr>
<td>Dependency Views</td>
<td></td>
<td>Level 1</td>
<td></td>
</tr>
<tr>
<td>Edge Encryption</td>
<td></td>
<td>Data only</td>
<td>Architectural support only.</td>
</tr>
<tr>
<td>Encryption Support</td>
<td></td>
<td>Data only</td>
<td></td>
</tr>
<tr>
<td>Flow Designer</td>
<td></td>
<td>No support</td>
<td></td>
</tr>
<tr>
<td>Homepage Administration</td>
<td></td>
<td>Data only</td>
<td></td>
</tr>
<tr>
<td>Integrations with third-party applications and data sources</td>
<td>Data only</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Knowledge Management</td>
<td></td>
<td>Level 2</td>
<td></td>
</tr>
<tr>
<td>Managed Documents</td>
<td></td>
<td>Data only</td>
<td></td>
</tr>
<tr>
<td>MetricBase</td>
<td></td>
<td>Data only</td>
<td></td>
</tr>
<tr>
<td>Mobile</td>
<td></td>
<td>Data only</td>
<td></td>
</tr>
<tr>
<td>Notifications</td>
<td></td>
<td>Level 2</td>
<td></td>
</tr>
<tr>
<td>Orchestration</td>
<td></td>
<td>Data only</td>
<td>Additional support possible, but depends on use case.</td>
</tr>
<tr>
<td>Password Reset</td>
<td></td>
<td>Level 2</td>
<td></td>
</tr>
<tr>
<td>Platform Security</td>
<td></td>
<td>Level 1</td>
<td></td>
</tr>
<tr>
<td>Schedules</td>
<td></td>
<td>Level 2</td>
<td></td>
</tr>
<tr>
<td>Service Portal</td>
<td></td>
<td>Data only</td>
<td>Architectural support only.</td>
</tr>
<tr>
<td>Product Suite</td>
<td>Application</td>
<td>Support level</td>
<td>Notes</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------</td>
<td>---------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>State Flows</td>
<td>Data only</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subscription Management</td>
<td>No support</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Survey Management</td>
<td>Data only</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time Card</td>
<td>Data only</td>
<td></td>
<td>Can be separated with customization.</td>
</tr>
<tr>
<td>Virtual Agent</td>
<td>Level 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Visual Task Boards</td>
<td>Data only</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workflow</td>
<td>Data only</td>
<td></td>
<td>Additional support possible, but depends on use case.</td>
</tr>
<tr>
<td>Performance Analytics and Reporting</td>
<td>Dashboards</td>
<td>Data only</td>
<td>Architectural support only.</td>
</tr>
<tr>
<td>Performance Analytics</td>
<td>Level 3</td>
<td></td>
<td>Can be domain separated, except for separated properties.</td>
</tr>
<tr>
<td>Reporting</td>
<td>Level 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Operations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Incident Response</td>
<td>Level 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat Intelligence</td>
<td>Level 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trusted Security Circles</td>
<td>Level 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability Response</td>
<td>Level 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Management - Other</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coaching Loops</td>
<td>No support</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facilities Service Management</td>
<td>Data only</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Finance Service Management</td>
<td>Data only</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legal Service Management</td>
<td>Data only</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Marketing Service Management</td>
<td>Data only</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Planned Maintenance</td>
<td>Data only</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Management Core</td>
<td>Data only</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Structured Problem Analysis</td>
<td>No support</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software Asset Management</td>
<td>Software Change Management</td>
<td>No support</td>
<td>Only the alm_asset table is domain separated.</td>
</tr>
</tbody>
</table>

**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>
<tbody>
<tr>
<td>domain_admin</td>
<td>Can create, edit, and delete domains.</td>
</tr>
</tbody>
</table>

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 to support the New Ticket module. 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>Options</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business rules</td>
<td></td>
<td></td>
</tr>
<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 -</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>Task</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain - Cascade Domain -</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>User</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain - Cascade Domain -</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>Version</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain - Deactivate</td>
<td>domain</td>
<td>Deactivates related companies if a domain is deactivated.</td>
</tr>
<tr>
<td>Companies</td>
<td></td>
<td></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 - 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>Companies</td>
<td></td>
<td></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>Name</td>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------</td>
<td>-------------</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>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>
</tbody>
</table>
### Domain basics

With domain separation (also known as ServiceNow Multi-Tenant Platform Architecture) you can segregate application data, User Interface, and business logic in a single customer instance, and support hierarchical modeling with cross-tenant intelligence.

Before you set off on the domain separation adventure, here are some basic good practices to follow. Select topics as you want or follow them in order by clicking the links below or from the navigation section at left.

### Domain separation recommended practices for service providers

The recommended practices section can help you more successfully create, implement, and maintain domain separation for your applications and services.

---

<table>
<thead>
<tr>
<th>Name</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>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>
</tbody>
</table>

### Business Rules Installed with Domain Support Plugin

<table>
<thead>
<tr>
<th>Name</th>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>(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>
What is domain separation?

With domain separation you can segregate application data, UI, and business logic in a single customer instance, and support hierarchical modeling with cross-tenant intelligence.

Domain basics

Domain, separation, aka ServiceNow Multi-Tenant Platform Architecture, adds considerable overhead to the management of an instance, but if used correctly and for the right reasons, it can improve efficiency, add greater security, and increase performance, improving the overall experience and management.

There are global standards and properties (such as system properties and table schema) that cannot be separated per tenant and must be considered globally for all customers.

Before setting off on the domain separation adventure, we recommend some basic good practices.

Features of domain separation

- **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.
  - Data records, when updated, do not generate Update Set records.
  - Users, including service accounts used for integrations, see only data in domains based on their visibility settings.
Typically, customers, agents, and fulfillers see data that pertain to customers and organizations they support.

**UI Separation**: Supports a tenant-specific experience for UI elements such as views, lists, labels, and so on.

The browser-based user interface, including application menus, lists, forms, homepages, and dashboards may be overridden and customized for a specific domain or set of domains while preserving baseline process logic.

Service providers can alter the displayed branding and UI elements to meet individual customer needs.

**Business logic Separation**: The creation of 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 have access to child tenant resources. Business logic for parent tenants runs automatically for child tenants, and can be overridden at any level.

**Cross-Tenant Intelligence**: Automatically handles data, metadata, business logic, and processing context for tenants with access to additional tenant data.
At a glance

What is 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 separation value proposition

Domain separation is designed to give service providers a multi-tenant instance architecture that delivers offerings efficiently and securely to their clients. Strong universal process standards, data-driven process design, strict governance, and centralized administration maximize these benefits.

Benefits

Domain tenants benefit from a quick return on investment, lower administrative overhead, and leverage of business services provided by instance owners.

Here is an "at a glance" 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>
</tbody>
</table>
### Definition of domain separation

With domain separation (aka the ServiceNow® Multi-Tenant Platform Architecture) you can segregate application data, UI, and business logic in a single customer instance, and support hierarchical modeling with cross-tenant intelligence.

#### Definition of domain separation

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.

#### How domain separation works

A common analogy for understanding domain separation is that 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, a pool, and so on.

With an apartment complex, someone else decides all of those things. Sometimes you can’t even paint.

---

<table>
<thead>
<tr>
<th>Instance Owner</th>
<th>Domain Tenants</th>
</tr>
</thead>
<tbody>
<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 the latest releases</td>
</tr>
<tr>
<td>Data segregation</td>
<td>Services provided by instance owner</td>
</tr>
<tr>
<td>Global reporting</td>
<td></td>
</tr>
</tbody>
</table>

© 2019 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.
Single vs multiple

Single
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.

- Higher upfront costs and administrative overhead, but more freedom to remodel and expand.
- 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 ServiceNow recommended practices and standards.

Multiple
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.

- A centralized staff administers configurations, integrations, and upgrades.
- Instance owner provides added services.
- Domain tenants have lower upfront costs to use ServiceNow, have lower monthly costs because they are sharing it amongst many tenants, and do not have to employ a staff to administer the environment.
- May also benefit from requests or changes initiated by other tenants.

Summary

<table>
<thead>
<tr>
<th>Domain separation attributes at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single-Family Home</td>
</tr>
</tbody>
</table>

© 2019 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>Mortgage</th>
<th>Instance costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner responsible for maintenance / utilities</td>
<td>Staffing to maintain</td>
</tr>
<tr>
<td>Can remodel and expand</td>
<td>Can add Integrations, functionality</td>
</tr>
<tr>
<td>Must comply with zoning laws</td>
<td>Comply with Support guidelines</td>
</tr>
<tr>
<td>Apartment Complex</td>
<td>Domain-Separated Instance</td>
</tr>
<tr>
<td>First and last month’s rent</td>
<td>Shared costs</td>
</tr>
<tr>
<td>Restrictions on remodeling</td>
<td>Process and apps pre-configured</td>
</tr>
<tr>
<td>Maintenance &amp; amenities</td>
<td>Instance owner sets roadmap</td>
</tr>
<tr>
<td>Fully or partially furnished units</td>
<td>Instance owner administers</td>
</tr>
</tbody>
</table>

**Domain separation hierarchies**

Hierarchies are a good practice for starting points in defining a domain architecture.
Sample domain separation hierarchies

In the Default domain, tasks

- In this example TOP is a process domain. It should never contain users, but should contain new process developed by the instance owner and overrides to processes as needed from global.
- **Default** is a data domain that only the service provider (SP) has access to. It should never contain active users, only lost data that should be reassigned to a proper domain.
- Tasks and users without a domain are placed here when created or updated. The behavior can be overridden by either un-checking the **Default** field on this record or 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.
- Moving data between domains is not a common practice and generally should not occur when using the instance.
- If any data is ending up in Default there is a configuration or procedural problem to be addressed.
• You do not see Global here as there is no global domain; Global is the absence of a domain on a record.
  • For example, a table with no domain field contains all global records, and on a table that has a domain field, any record without a domain is global.

• You will see the word Global in the domain field. It is placed there auto-magically when the record has no domain.
• Not accounting for the security model, global records are available to all users of the instance.
  • For this reason the Default domain is recommended to make sure records do not end up in Global on tables that should never have global records.
  • The instance owner must then triage records in Default and move them to the correct domain.

Domain Hierarchy

• Parent/child – Process and Data affected
  • Primarily designed based on process flow, but keep in mind that parent domains have access to all data in child domains

• "Contains" domain – Only data is affected (for example, making MSP in the example above contain TOP does not make processes in MSP run in TOP and below).
  • Used to grant data access rights to individuals in groups that require dedicated access to certain domains
  • Use only as needed, contains causes or conditions to be added to DB queries that can cause performance issues with large domain and or data sets

• Visibility – Always visible once granted, only data is affected
  • Used to grant data access of a domain to another domain that did not gain that access when building the parent/child hierarchy
  • Use visibility sparingly: It breaks some of the intelligence model by allowing users to see all data in domains they are granted visibility to, all the time, regardless of the record they are working on.
Unrestricted/Restricted Use Cases for Domain Separation

Many SPs often have customers who implicitly state that access to their domains must be tightly regulated, which constrains the use of “Contains” at the TOP domain. Here is how to handle such a use case:

- 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**;
  - With customers who do have that requirement, place them and their domains under **Restricted**.

- System admins can then leverage “Contains” and “Visibility” functions in an efficient, targeted manner.
  - “Contains” is applied to **Unrestricted**, so a single “Contains” can grant visibility to most customers.
  - Domain visibility is applied using “domain visibility groups” to specific domains as needed.
Tasks and users without a domain are placed in this domain when created or updated. This behavior can be overridden by:

1. Un-checking the Default field on this record
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.

**Domain separation architecture data**

Based on the domain hierarchy, users have access to data in their home domain and any child domains. The process flows down and the data bubbles up.

**Domain architecture**

User records are assigned a domain value, which 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 and domain visibility](#) for advanced options to grant additional domain visibility.

**Domain Architecture: Process Flows DOWN**

```
Base Instance (global)

Parent Company Domain

North America

Organization 1

Organization 2

Organization 3

EMEA

```

© 2019 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.
Context and domain separation

The context of a user’s session determines processes, data, and UI as they browse list views, home pages, reports, and knowledge articles.
User session context

The user in this example has a home domain of Cloud Dimensions.

1. The branding reflects settings in the Cloud Dimensions domain and company record.

2. The navigation menu shows items inherited from higher-level domains as well as modules defined in the Cloud Dimensions domain.

3. Home pages and list data reflect data that is visible based on the user’s session context. In this case, the user in the Cloud Dimensions domain can see data in Cloud Dimensions, child domains, and global.
User session context starts in the home domain

Users’ home domains are set 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 context of the user session includes home domain as well as any child domains. This set of domains in the user’s session context is automatically appended to every query sent to the database. That way the results are limited to just the data in these domains and global data. The logic controlling this is embedded in compiled code that is not accessible for manipulation through the application.

Service accounts used for integrations also have user session context. Database queries are limited in the same way as interactive users.

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.

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 regardless of the user’s domain.
- Records can be viewed concurrently in multiple browser tabs maintaining their own record context.

Segregate and secure domain separation data

There are multiple ways to segregate and secure data on the ServiceNow platform, depending on the breadth and depth of the customer need.

© 2019 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.
Multiple methods of data segregation

1. If departments or groups need to focus on work that pertains to them, using advanced reference qualifiers and filters may be sufficient. In this case, the consequences of one department or group seeing another’s records is low.

2. Contextual Security and Before Query business rules offer additional layers of security to guard against data breaches.

3. Domain separation adds another level of security, ensuring data returned from every database query is limited to data based on domain visibility before Contextual Security and business rules are executed.

4. For absolute segregation at the database and application layer, you may want to consider separate instances.

Not all organizations require domain separation. Depending on what the customer needs for separation and the consequences of data breaches, other alternatives may suffice.

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.
## Separate instances

**Separate Instances**

- **Pros**
  - Build to suit each customer/organization
  - Minimize impact of customizations on others
  - Release schedule coordination
  - Clean separation
  - Choose data center region

- **Cons**
  - Cost
  - Alignment amongst instances
  - Testing effort for upgrades
  - Duplication of effort
  - Integrations required

**Single Instance – without Domain**

- **Pros**
  - May address simple scenarios
  - Cost

- **Cons**
  - Extensive modifications to baseline code
  - Modified baseline code skipped during upgrades
  - Must address all secondary & supporting tables as well
  - Extensive testing required
  - No ServiceNow product team to evolve your custom code

You can choose to time upgrades and releases so they are coordinated separately for each instance. However, separate instances also require a greater degree of coordination among the instance administration team. When you configure instances using contextual security, form views, reference qualifiers, filters, and robust conditions, these are also commonly considered as an alternative to domain separation.

This approach may address simple scenarios for data and process separation, but places the burden of maintaining and evolving extensive customizations with the instance owner.

### Evaluating the need for domain separation

Domain separation is not always the best route to go; it's best to base your decision on numerous discussions and evaluations.
**Indicators for Domain Separation**

These factors may indicate that domain separation is recommended.

- Customers have moderate alignment of processes and general platform requirements.
- Customers plan to work on tasks as fulfillers rather than as requesters.
- Contractual agreement require isolation of data records, but instance owner determines that the requirement may be addressed at the application layer.
- Instance owner has entire entities that operate as physically separate organizations and do not share data, yet global reporting and entity reporting is required.

**Indicators against Domain Separation**

These factors can point to reasons not to set up domain separation.

- Customers want to administer their environment, have full ownership of it, and set the roadmap for expansion.
- Customers require complete isolation of data and process at the physical or database level. (Domain-separated instances contain a shared database.)
- Departments want to isolate records. (Access controls may suffice.)
- Customers all want their own processes, business rules, and workflows.
- The corporate culture is one of non-collaboration between organizations.
- Customers interact with the platform as end users only.

**Advantages to domain separation**

There are clear advantages to domain separation. You must weigh your needs versus the benefits, as demonstrated in this topic.

**Advantages at a glance**

Domain Separation is enabled with a ServiceNow plugin with functionality built into the core platform. The functionality is managed by a product manager supported by a development team. Enhancements and fixes for domain separation functionality are included with ServiceNow releases and may be consumed by customers. Instance owners can use an array of ServiceNow Technical Support resources, such as the **Service Portal** for assistance with domain separation.

**Database query with domain separation**

Domain separation protects data and creates a more efficient performance.

**How domain separation protects data**

In this image, the Incident `[incident]` table has a domain field (inherited from Task). That means that the records in the table can have domain assignments.
When users log in, their home domain is identified along with the set of domains they may access. This is known as the user’s session context.

1. In the browser, the user clicks the **Open Incidents** module to view incidents where Active = true.
2. The filter is submitted to the application.
3. The application sends a query to the database appending a WHERE clause to limit the incident records returned to those in the user’s domain or domains they may access. Only records in these domains are returned to the application for processing.
4. Contextual Security is applied, further limiting the data returned to the user. The incident records display in the Open Incidents list.

To learn more about Contextual Security see **Context and domain separation**.
**Domain separation levels of support**

There are four high-level considerations for domain separation of an application. These levels are explained in more detail in this topic.

ServiceNow applications are defined in the domain separation support level system, which operates from the perspective of actual use cases and personas.

### Incremental support levels

<table>
<thead>
<tr>
<th>Level</th>
<th>Type</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Data only</td>
<td>- The tenants of the instance can use the application without being aware of other tenants due to the domain field on the applications tables. But the instance owner has not created logic to route the data to the proper domains for all use cases. This level is not considered truly domain-separated.</td>
</tr>
<tr>
<td>1</td>
<td>Tenant Data Management</td>
<td>- The owner of the instance needs to be able to set up the application to function normally across multiple tenants. Data routing to domains should be handled natively by the application for all applicable use cases.</td>
</tr>
</tbody>
</table>
| 2     | Tenant Process Management        | - 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. |
| 3     | Tenant Self-Managed Configuration | - The tenants of the instance need to be able to:  
  - configure MVP business logic and data parameters for themselves that would be expected for the application's normal function. |

Domain separation is a framework that you have to use to make your applications tenant-aware.

What to understand: 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

The Service Provider (SP) reference architecture is designed so that customers can access SP services via a portal to their domain-separated instance.

**SP Reference Architecture – Domain Separation**

- SP customers access SP services via a portal to the SP Domain Separated instance
- SP uses ServiceNow shared instance(s) to manage their service delivery
- SP could have a shared instance per region to support data sovereignty requirements

Legend:
- Centralized governance at the SP
- Centralized administration at the SP, Shared business requirements and configurations
- Both SP and customer fulfillers on one instance
- Customer requesters on each instance

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.

**Attributes**

- Fulfillers are not assigned to a domain, fulfillers are SHARED across domains so it is nearly impossible to audit the number of fulfillers per domain (for split adjustments).
- Administration is shared and leveraged so there is no overhead and the SP can optimize licenses.
- The number of users on the instance can change drastically as a new customer can result in tens or even hundreds of thousands of net-new users on the system immediately at Go-
Live. That also means that the number of total users is virtually “unlimited” due to one shared environment.

Reference hierarchy for domain-separated instances
### SP reference architecture comparison

**Service provider reference architecture decision tree**
Service Providers use dedicated instances to manage their service delivery. Use the decision tree and comparison chart to help you determine if a new customer should be added to the shared instance or to their own dedicated instance.

<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>

© 2019 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.
Dedicated vs shared

- Physical sep required
- Logical sep is OK
- Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware
- Customer wants full power of platform to solve needs outside of SP
- Customer requires many processes or services not offered by SP
- Customer wants to administer own process

Dedicated
Service provider reference architecture comparison

<table>
<thead>
<tr>
<th>Standalone (SA)</th>
<th>Multi-Tenant (MT)</th>
<th>Hybrid (MT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform as a Service</td>
<td>Enterprise scale</td>
<td>Processes simplified</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>
</tr>
</tbody>
</table>

Service provider reference architecture – Dedicated Instances

The dedicated instances Service Provider (SP) architecture is designed so that SP customers access their services via 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

- Administration is separated and has dedicated teams for each instance. Administrators or developers who must log into multiple instances require multiple licenses.
- Each instance has a finite number of users (both requesters and fulfillers). A net-new customer is defined for size and scale and the instance is procured appropriately.
Dedicated vs. Shared

- **Physical sep required**
  - **Logical sep is OK**

  - **Large customer:** Transactions or data amount stored cause for multiple nodes or dedicated hardware

- **Scale**

  - **Standard customer:** Expected to consume managed services on shared instances

- **As a Platform**

  - **Customer can work within products & services of SP**

  - **Customer wants full power of platform to solve needs outside of SP**

  - **Customer requires many processes or services not offered by SP**

- **Process Diff**

  - **Customer can stay within 95% of delivered services**

  - **Customer wants to administer own process**

  - **Customer needs to consume only managed services**

- **Administer**

  - **Dedicated**

  - **Shared**
## SP reference architecture comparison

### Service provider reference architecture – Hybrid

The hybrid Service Provider (SP) reference architecture provides a customized solution. The SP customers require a dedicated instance for a specific service. They can still use the shared SP instance for other services, but it requires integration.

### The hybrid architecture

The SP customer may be responsible for delivering this additional service directly.
Attributes

- The administration of the instance is shared and leveraged so there is no overhead, and the SP can optimize licenses.
- If there is a net-new instance for a de-centralized environment, the program team is responsible, and funded accordingly as dedicated administrator users for that instance. For a centralized environment such as HCL where all instances stem from a blueprint, duplicate administration licenses are required.
- Fulfillers are not assigned to a domain, they’re shared across domains. So it’s nearly impossible to audit the number of fulfillers per domain (for split adjustments).
- If a resource is shared and supports a customer on the shared environment and a dedicated environment, that user requires a fulfiller in both the shared and the dedicated environment. It is also a productivity hit as processes are typically different from the shared instance to the dedicated instance.
- The number of users on the instance can change drastically as a new customer can result in tens or even hundreds of thousands of net-new users on the system immediately at Go-Live. Also, the number of total users is virtually “unlimited” since this is all on one shared environment.
- The dedicated instance has a finite number of users for scale.

<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>

**SP reference architecture comparison**

*Service provider reference architecture – SIAM*

The Service Integration and Management (SIAM) for service provider (SP) architecture integrates services for a unified customer experience.
SIAM architecture at a glance

**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.

**Attributes**

- SP customers access SP services on a dedicated or shared portal to the SP shared instance.
- SPs useServiceNow shared instances to manage their service delivery.
Domain separation terms and conditions

Domain separation adds considerable overhead to the management of a ServiceNow instance. But if you use it correctly, and for the right reasons, domain separation can improve efficiency, add greater security, and increase performance. This topic focuses on terms and common configurations to help you get an improved overall experience and smooth management.
Managed domain

- **Common Use Cases**
  - Set admins to ‘global’
  - Set support groups to ‘global’

- **UI Policy shows Domain when Managed domain = true**

<table>
<thead>
<tr>
<th>Tables with managed_domain</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User</strong> [sys_user]</td>
</tr>
<tr>
<td><strong>Group</strong> [sys_user_group]</td>
</tr>
<tr>
<td><strong>Configuration Item</strong> [cmdb_ci]</td>
</tr>
</tbody>
</table>
In process tables, when the `Overrides [sys_overrides]` field value is present, a process override record exists. That means that delegated administration is in effect. Admins in global can use Expand/Collapse Domain Scope Related Links to see override records.

**Note:** Reports are domain-separated and contain an `Overrides` field. To view all reports from global, use the Expand Domain Scope control.

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 global, Expand Domain Scope is available. All process records, including overrides, are visible when Domain Scope is expanded. To view only relevant process records for the global again, use Collapse Domain Scope.

This 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 process to flow down to children.
Customer, process, and data domains, and user data

Domain hierarchy

Customer Domain
- UI, processes, and data for a single customer
- Example: ACME on the sample domain hierarchy

Process Domain
- Specific processes and UI settings for a set of domains
- No core data of any kind belongs here (for example, users).
- “TOP” in the sample hierarchy is a process domain.

Data Domain
• Domain that holds data relevant to multiple customers that can be shared, without sharing each other’s customer domains. The domain is contained by each customer who needs access to it. 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.

• “Default” in the sample hierarchy is a data domain.

User Data
• User record data never belongs in global 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 global to facilitate administrative functions.

Choice lists, admin, global process

Choice 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 choice field. If the new choice is marked as Selected, it is added as active, and if the new choice is marked as Available, it is added as inactive.

Instance Administration
• All normal process creation, modification, and maintenance in a domain-separated instance has to be handled by the instance owner’s administrators. Some data-driven pieces of processes can be maintained by individual domain managers such as user administration, support group memberships, and locations, or when an application has been specifically designed with tenant administration in mind.

Global process/parameters: Common to all users of a domain-separated instance. Examples:
• System properties, dictionary overrides, sys_documentation (field labels), the data model (classes, CI types, etc), 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.

See

Domain-separate a custom table

Custom tables may need to be domain-separated. This topic covers both the procedure and the concept behind domain-separating a custom table.

1. Create a sys_domainfield

If a system table or a table has not been domain-separated by the Domain Separation plugin, it’s best not to domain-separate it.
• Create a new field and leave it as a string.
  • Column Name: sys_domain
  • Other attributes: Defined automatically

• Sys_domain_path is created automatically

The column name “sys_domain” is reserved in ServiceNow. The system recognizes it and applies special handling to set the appropriate field type and attributes. The special handling also creates a corresponding sys_domain_path field.

---

**Note:**

• Be sure to set the Column Name to sys_domain rather than the label.

• Domain separation is not appropriate for EVERY table. In general, if a table is part of the base instance and that table does not have a sys_domain field, it is STRONGLY recommended that you leave it that way.

A sys_domain is created automatically when you create a string field with the name “sys_domain” on a table.

---

2. Add a business rule to set domain

**Without business rules**

• Domain is set to the current domain of the user who creates the record.

**With business rules**

• Domain is assigned using scripted logic, typically based on Company.
In addition to a `sys_domain` field, custom tables need a business rule similar to `Domain - Set Domain - Task` to set the value of the domain field. In addition, you will need `Domain - Default - Task`, which moves records without a domain to the default domain if the first rule fails to assign a domain.

On the task table, review the business rules for Domain. Pay particular attention to the Order field.

The first rule that runs, `Domain - Set Domain - Task`, attempts to set the domain of the record based on the record’s Company’s Domain.

If the first rule fails to find an appropriate domain, the second rule, `Domain - Default - Task`, executes. This rule sets the domain of the record to the default domain.

Finally, if the domain of a task record changes, the `Domain - Cascade Domain - Task` business rule changes the domain on all records related to the task, such as workflows, metrics, SLAs, and attachments.
3. Domain – set domain – default
If the initial business rule fails to set a domain and Domain is still empty or global, a second business rule runs. This rule examines the task_for field (set based on caller or requested_for) 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.

4. Domain – cascade domain – task

Tasks do not work alone!

Tasks may have a number of 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 users in the new domain.

This rule is commonly triggered when clearing records out of the Default domain.

Domain properties and themes

Service providers can customize their customers’ Company properties and themes. These are the recommended practices for domain properties, themes, and the Company setting domain.

Domain properties page

Use the domain of the record being viewed instead of the user’s own. When true, the admin can then run under the domain-specific processes of different domains even if working from a common list.
Company themes

On the company record, each company can have specific theming and logos.

Company sets domain on Task, User, Group, Location, Department, and CMDB

By default with the Service Provider plugin installed, there are business rules on core tables that cause the records domain to be set to the domain of the company associated with the record. This is recommended practice and should be replicated as new core tables are created.

There is no reason for anyone other than admins to see the domain field on these tables.

All of these tables, except Task, have a Managed Domain flag that can be set to override the domain a record is created in.

Emails, catalog, users, groups, views, and tables

Use these recommended practices for domain-separating email notifications and customizing the properties of catalog, tables, users, groups, and views.

Emails

Email notifications are domain-separated and override-capable. When domain-separating notifications, the overrides function based on the domain of the attached record, not the user’s domain. (ITIL User in MSP domain, Task in ACME, The notification sent is the ACME override)

Service Catalog

The Service Catalog is not domain-separated. Use entitlements, entitlement scripts, and roles for visibility and access. Entitlements are processed as "OR" conditions when multiples are used. Categories and Items should be administered by the service provider.

Users and groups

Only admin accounts should exist in the global domain. Do all your application testing from an actual domain and not in global because overrides do not process properly in global. Admins should be given user accounts in production if they are to use the application.

Forms, lists, fields, tables, columns

- Lists – Pay close attention when troubleshooting lists because there are Personal, Global, and Domain lists, as well as multiple views of each.
- Forms – Pay close attention when troubleshooting forms because there are Global and Domain lists as well as multiple views of each.
- There is only one database, so any fields created exist for all, and should be considered globally before you create one.
  - ACL scripts cannot keep a field from being viewed in a list because they do not run. A READ ACL can hide a field from users if the ACL is only role-based.
Creating tables – Every time you create a table, consider if it needs a `sys_domain` or `sys_overrides` field. Any table that holds data that instance users need to access, needs `sys_domain`. Tables that extend or support process and need to flow down to children domains also need `sys_domain`.

Domain picker and configuration process
Use the domain picker wisely, and remember the 80/15/5 approach.

Verify your domain before making changes
If your session times out, even if you do not 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 you selected if the top frame has not been reloaded. For this reason it's best to reload your tab completely if you have been away from the instance for any time.

The 80/15/5 approach: Configure at the TOP domain or Global
Domain separation works best when providing services to customers that are mostly standard. Variations in process for services should be delivered in properties that work automatically for each customer, but can be adjusted as needed. Use great care when deciding when, and to what degree, tenant configuration should be approved for a single customer.

- Recommended approach:
  - 80% or more Standard
  - 15% or more Parametric
  - Less than 5% Configuration

- Do not write process in a vacuum. Always put on your "global" hat to determine if a suggested change should be global, or a configurable property.
- Do not overbuild (KISS)

1. Start with base system features and verify gaps before making changes.
2. Look for no-code solutions.
3. Use server-side scripts, build modular APIs, and build in domain-separated properties.
4. If you must use client scripting, use only ServiceNow APIs and limit AJAX, especially synchronous calls.
   - Write all scripts logically to “Get out quick.” Enforce peer reviews of code changes and make sure everyone is following recommended practices.

Performance considerations
As you configure domain separation in your application and services, make sure you consider everything that can impact performance.
Limit the number of domains

Admins can create as many domains as needed, but make sure you do not create unnecessary domains on the instance. Why? Because everything comes with a price, and a large number of domains on the instance can impact performance.

For example, too many domains can slow down the domain picker, and that slows down the overall user experience. Specifically, if you are loading domain picker on the header and have a large number of domains, the domain picker has to load all domains before giving the user control in the session. This could lead to an outage: The user is unable to access anything on the instance until the domain picker finishes. Before creating new domains, check the domain hierarchy under Domain Admin -- Domain Map and make sure you actually need to create a new domain, or whether existing domain hierarchy will work.

Use the UI16 domain picker

Domain reference picker available in UI16: With the reference picker, you do not load all the domains at once, but rather the domain is searched as the user types into the domain picker. This gives better performance when the user logs into the instance.

Enable the domain reference picker in UI16 by following these steps:

1. Enter sys_properties.list in the application navigator.
2. Set the following property to true: glide.ui.domain_reference_picker.enabled
3. Refresh the browser.

Note: Do not upload a large number of domains via integration or import sets without testing or you can bring down your instance.

Domain hierarchy

You can avoid slowdowns and glitches by knowing how domain hierarchies work and setting them up properly.

Make changes to the existing domain hierarchy only when absolutely needed. Once you've created the domain hierarchy it's best not to keep changing it. When you update the parent of a domain, the system re-parents all the related domains that change the domain hierarchy. When the domain hierarchy updates, the system triggers a cascade update on all domain-aware tables for the records created on that domain. As a result, it's not just one table updating, it's a large number of other tables in the backend, too.

For the same reasons, even if it's absolutely critical to change the domain hierarchy, never do a mass update. Imagine the number of queries the system has to run to change the domain hierarchy. Always do an update in small batches, and before starting the next batch, make sure Domain Work Request (DWR) records are processed.

How to track DWR records

In the syslog_domain table, there is an information entry for DWR execution completed. Always look for this entry to confirm that DWR is completed.
Domain logs for errors and warnings

Domain logs can help you find errors or warnings in your processes and configurations.

Always check domain logs for any errors or warnings. Domain logs are stored in the `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.

The system also captures the logs in the table when the domain validator runs and domain paths are recalculated. Look for any errors and warnings in this table. After reviewing this table, admins need to resolve these errors and re-run the domain path validator.

Here is an example of how the logs look:

<table>
<thead>
<tr>
<th>Level</th>
<th>Message</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DomainWorkRequestExecutor worker thread pool is shut down. Total time</td>
<td>com.glide.domain_pal</td>
</tr>
<tr>
<td></td>
<td>taken for executing the threadpool : 0:00:20</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Information</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DWR execution completed</td>
<td>com.glide.domain_pal</td>
</tr>
<tr>
<td></td>
<td><strong>Information</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DomainPathUpdater is finished! Total time taken for migration : 0:00:20</td>
<td>com.glide.domain_pal</td>
</tr>
<tr>
<td></td>
<td><strong>Information</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>All DWRs have been processed. Producer will shutdown consumers and exit.</td>
<td>com.glide.domain_pal</td>
</tr>
</tbody>
</table>

In this image, 10 orphan records in the `sys_ui_list` table are detected. An admin must fix these records in order to run the domain path validator successfully.

To learn more see [Troubleshoot domain separation errors](#).
Importance of the Default domain

Keeping your domains organized is a crucial part of the domain separation process. Make sure you know the importance of the Default domain.

Always have one Default domain set 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.

Create a default domain with the name Default to differentiate it from other domains and check the Default check box. Here is what your default domain configuration will look like:

If you don’t set a default domain, new tasks and user records then go to the global domain. Anyone can see the records in the global domain, meaning data can be seen when it isn’t supposed to. If you set the default domain, its records are not visible to any user other than an admin.

However, admins should regularly maintain records created in the Default domain and move them to the correct domains. If records show up often in the Default domain, admins may need to investigate why. Ideally, you should make sure all records are created in their appropriate domains (not global or default domains).

Contains and domain visibility

"Contains" is a domain-to-domain relationship that is many-to-many, and has no effect on the flow of process. Creating domain contains and user or group visibilities for a domain should be an exception, used only when absolutely needed. This topic explains why.

Use domains-contains and user or group access only in special cases. One such case would be when a user or group needs to see the data from a domain that they don’t have access to, but moving those users or groups is not an option.

A large number of domain contains or visibility generates queries with too many "OR" conditions, which are slow and impact performance. Rather than using too many contains relationships, set up your domain hierarchy correctly.
This query is for just one contains relationship. If you have a domain contain another domain, which is the parent of a number of other domains, you will have many more “OR” conditions like this. It’s best to carefully create a Domain Map. Then, before moving the user to the domain, make sure the domain is appropriate for users to have all necessary access.

Note: You should not have too many domain contains and domain visibility set up on the 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 using domain path are much faster than spooling or numbering.

Domain path recently became the default query method for instances that had enabled domain separation, so if you are a fairly new customer, you don’t need to create one yourself. It’s the default for instances that enabled domain separation in Eureka and above.

However, if you are a long-term customer on domain separation and want to verify the query method on your instance, look for the following system properties:

- **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

These properties confirm your query method.

**Slow queries and SQL debugging**

Debugging SQL can help you resolve slowness issues in an instance.

When admins debug an instance, they can enable SQL Debugging to look for slow queries. Another way to look for slow queries is to check the Slow Queries [sys_query_pattern] table by navigating to System Diagnostics > Stats > Slow Queries. This table stores slow queries in the instance.

You can search the table for, say, queries that contain domain_path to determine if there are any slow queries due to domain path in your instance.

If you do find slow queries, try to analyze why they are slow.
Common reasons for slow queries

- Too many "OR" conditions (as discussed in Contains and domain visibility): In the domain hierarchy, see if you can place the user or a domain at a hierarchy level where contains or visibility is not needed.
- Query method is not domain path (discussed in Domain paths query method): If you are not using domain path query method, contact ServiceNow Technical Support.
- Query needs indexing: If you are able to identify the slow query, run the "explain plan" to see if there are options for indexing available.

About Before Query business rules

You can use a 'Before Query' business rule to help support data segregation.

A "Before Query" business rule is supplementary server-side code that system administrators can use to support data segregation within their domain-separated environments.

**Warning:** This method must never be used to avoid using the Domain Separation plugin. This business rule doesn't perform as well nor is it as secure in preventing data leakage.

Before Query for data segregation

There are certain situations where Before Queries can work with data segregation:

1. When domain separation is not supported by a ServiceNow application AND table or row access must be granted or restricted to one or more non-internal customers outside of the service provider organization

   **Note:** Prior to beginning development, ask a ServiceNow representative about the application roadmap for that product; there may be domain support improvements planned for upcoming releases.

2. 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
   - Example: A customer in "X" domain has multiple vendors supporting their domain and those vendors are granted access to see only records assigned to them

Points to consider

Before Query business rules can be scripted thoughtfully 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 domain-separated and can be created to apply globally, or more appropriately, 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 whom it applies.
- 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. (Example: Transform Maps with "Run" business rules turned off, or scripts with workflow disabled, and so on.).
• Always populate the condition field to specify when the rule runs (for example, if it applies only to certain vendors in a domain).

**Warning:** When designing and coding business rules (especially Query business rules) make sure the code is efficient by limiting “OR” clauses and searching non-indexed fields. Otherwise, you can cause slow queries or serious performance impact on the instance.

• Like salt on food, use Before Queries only when necessary; too many of these types of rules can impact performance.

• Before Query business rules fire before ACLs and perform better in general; this is especially true when limiting the returned results to users in SP environments who may have access to several domains in the system.

• In the user experience the data filtration is totally transparent (unlike ACLs) to users who will not see the message Data Security restricts... when interacting with data.

### When not to use Before Queries and ACLs

**Technical debt:** Using Before Queries and ACLs to segregate customer data creates customizations that must then be maintained, potentially causing performance issues. Teams should provide processes to make sure they don’t break the system.

Domain separation provides both scalability and governance with the current domain “path” query method (v3), a widely supported framework that the ServiceNow Platform and App teams - not the customer - are responsible to maintain.

**Performance Issues:** In large customers, excessive use of Before queries and ACLs get to a point where database queries don’t perform well.

### A little context

Domain separation started out using un-cached queries (v1) to separate companies. As service providers’ customers’ needs grew in complexity, that process evolved into cached (spooled) queries (v2), and then to new performant query methods required to handle the load.

Domain separation is enabled with a ServiceNow plugin with functionality built into the core platform. 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 ServiceNow Technical Support resources such as the Service Portal for assistance with domain separation.

### Don’t use domain path in scripts

Domain paths can cause the values of your script to change so it's best not to use them in scripts.

Your script should not depend on the domain path. Should you ever change the domain hierarchy, the domain path recalculates and its value changes. If this happens, your scripts are useless or can throw errors. The best strategy is not to write your scripts on the basis of domain path.

Always use the `sys_domain` field in your scripts to determine or evaluate the domain. Look for base system business rules, which use the `sys_domain` field, to get some ideas before creating your own scripts.
Domain assignment

How you assign the domain impacts the value of the sys_domain field.

Value of the sys_domain field

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

Make sure that domain assignment strategies and design are well documented and tested so that as records are created they are inserted into the correct domain.

Domain separation and the Customer Service Management plugin

For the best outcome, be aware of how the properties in the CSM plugin work.

Instance owners are advised to turn on this property:

- csm_auto_account_domain_generation
- Value: true

**Note:** This is the base system property that is available after CSM plugins are enabled.

1. What does this property do?
   - 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 new account as a sub-domain of the parent.

2. What happens if this property is not true, and domain is enabled?
   - New account records in a domain-separated environment are automatically placed in the Default domain.
Domain separation setup and basic 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. Access the Domain Configuration console
3. Create a domain
4. Add a user and a record to a domain or Add a domain field to a table

You can also perform these basic administrative tasks on domains:

- Activate or deactivate a domain
- Use a custom table for the domain table
- View domain relationships
- Change domain visibility
- 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: none

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. ServiceNow Technical Support can assist in the upgrade.

1. In the HI Service Portal, click **Service Requests > Activate Plugin**.
2. Fill out the form.

<table>
<thead>
<tr>
<th>Target Instance</th>
<th>Instance on which to activate the plugin.</th>
</tr>
</thead>
<tbody>
<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>Date and time must be at least 2 business days from the current time.</td>
</tr>
</tbody>
</table>

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

| Reason/Comments | Provide any information that would be helpful for the ServiceNow personnel activating the plugin. For example, if you need the plugin activated at a specific time instead of during one of the default activation windows. |

3. 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.

**Access the Domain Configuration console**

Use the Domain Configuration module to enable, configure, and view the status of domain separation support.

You can set domain separation configuration options, such as selecting the domain table and enabling delegated administration. You can also view domain alerts.

1. Navigate to **Domain Admin > Configuration**.
The Domains Configuration page appears.
2. Configure the following Domain Separation options:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Table</td>
<td>Shows the table containing domain names. By default, the system uses the Domain (domain) table. Click <strong>Change domain table</strong> to change the table.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Change domain table</td>
<td>Select the table containing domain names for domain separation. You can select any existing table. By default, the system uses the Domain (domain) table. Warning: No domain can have the name <code>global</code>. Verify that the name <code>global</code> is not used in any of the domain names in the table before saving the domain configuration.</td>
</tr>
<tr>
<td>Domain Validation</td>
<td>Shows the status of last domain validation run. Click Validate domains hierarchy to run Domain Validation. See the Domain Alerts section or the syslog_domain table to view any warnings or errors in detail.</td>
</tr>
<tr>
<td>Validate domains hierarchy</td>
<td>Run the domain validation. See Validate domain hierarchy.</td>
</tr>
<tr>
<td>Show tables with sys_domain field</td>
<td>Show all the tables with the Domain field. Lists all the Dictionary Entries of tables with the Domain (sys_domain) field.</td>
</tr>
<tr>
<td>Domain Progress Workers</td>
<td>Lists any currently running conversion or validation processes.</td>
</tr>
<tr>
<td>Domain Alerts</td>
<td>Lists any information, warning, or error messages relating to domain separation. You can also find this information in the syslog_domain table.</td>
</tr>
<tr>
<td>Enable Domain Separation</td>
<td>Select whether to enable or disable domain separation. By default, domain separation is enabled. You can manually disable domain separation with this setting. However, the sys_domain column will still be present on any table it was added to. This option maps to the glide.sys.domain.partitioning system property.</td>
</tr>
<tr>
<td>Enable Delegated Administration</td>
<td>Select whether to enable or disable delegated administration. Activating the plugin automatically enables delegated administration. You can manually disable delegated administration with this setting. This option maps to the system property glide.sys.domain.delegated_administration. This property controls process separation.</td>
</tr>
<tr>
<td>Enable verbose domain logging</td>
<td>Select whether to enable additional debugging information for domain separation. This option maps to the system property glide.sys.domain.verbose.</td>
</tr>
</tbody>
</table>

**Note:** When both glide.sys.domain.delegated_administration and glide.sys.domain.partitioning are disabled, all domains are disabled. Users logging in have their session domain set to `global`.  

© 2019 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.
Domain scope 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 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 scope 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`

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>
<tbody>
<tr>
<td>glide.sys.domain.skip_domain_insert_businessrules</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• Type: true</td>
</tr>
<tr>
<td></td>
<td>• Default value: True in new domain activations starting with Jakarta. False in existing implementations.</td>
</tr>
</tbody>
</table>

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>glide.domain.session_scope</td>
<td>Domain</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>
</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 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 Vendor, Customer, and MSP. 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>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>
</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.

**Add a user and a record to a domain**

By default, all users and records are part of the global domain and are therefore accessible to all users.

Role required: admin

To use *data separation* and *delegated administration*, you must first assign users and their relevant records to one or more domains.

1. Personalize the list or form to add the **Domain** field.
2. Set the **Domain** field for the user or record.

For example, assign Bow Ruggeri to the Network domain. Assign Don Goodliffe to the Database domain. Add the Network and Database domains to relevant records such as incidents, configuration items, requests.

**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**.
Tasks and users without a domain are placed in this domain when created/updated. This is done:
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.
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.

Activate or deactivate 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 custom tables by adding a sys_domain field to it.

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.

Note: Any other means of creating a field adds a u_ prefix to the column name. For domain separation to work the column name must be sys_domain without any u_ prefix.

Use a custom table for the domain table

You can use a custom table as the domain table if the custom table contains a reference field column called parent that refers back to the custom table.

Role required: admin

1. Create a custom table to store the domain information. For example:

<table>
<thead>
<tr>
<th>Table</th>
<th>Column name</th>
<th>Type</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>u_organization</td>
<td>u_name</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td>u_organization</td>
<td>u_description</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td>u_organization</td>
<td>u_location</td>
<td>reference</td>
<td>cmn_location</td>
</tr>
</tbody>
</table>

2. Create a reference field within the custom table that refers back to the custom table. For example:
3. Select the custom the table from the list of tables in the **New Domain Table** list.
4. Click **Reset Data** to make these changes:

   - The domain table changes to the table you selected.
   - All existing records with a domain value are reset to the global domain.
   - All existing domain overrides are deleted.
   - All existing domain contains definitions are deleted.
   - All existing domain visibility settings, both user and group, are deleted.

5. Click **Ignore Data** to make these changes:

   - The domain table changes to the table you selected.
   - All domain visibility settings, both user and group, are deleted.
   - All existing records with a domain value refer to invalid domains until you migrate the domain data.
   - All existing domain overrides refer to invalid domains until you migrate the domain data.
   - All existing domain contains definitions refer to invalid domains until you migrate the domain data.

**Note:** Visibility settings are deleted whenever the domain table reference changes.

When you select the ignore option, no existing domain-separated tables are moved to the global domain, and it is your responsibility to migrate the domain records. Until the migration is complete, the domain validator shows warnings about inconsistent domain...
data. If necessary, you can manually reset all domain-separated tables to the global domain.

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**.
<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>TOP</td>
</tr>
<tr>
<td>Type</td>
<td>MSP</td>
</tr>
<tr>
<td>Primary</td>
<td>Yes</td>
</tr>
<tr>
<td>Description</td>
<td>Top level, process flows down from here. Overrides from global process are done here.</td>
</tr>
<tr>
<td>Default</td>
<td>No</td>
</tr>
</tbody>
</table>

**Companies**

- **Domain = TOP**
  - Name: [Input Field]
  - Street: [Input Field]
  - City: [Input Field]
  - Zip / Postal code: [Input Field]
  - Phone: [Input Field]

**Contains Domains**

- **Domain = TOP**
  - Contains: [Input Field]

**Contained By**

- **Contains = TOP**
  - Domain: [Input Field]
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 visibility 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**.

Change domain visibility
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.
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 domain 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
You can add visibility domains for specific users on the User form.

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>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Inherited</td>
<td>Domain is inherited from domain visibility or a parent domain.</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 field 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**
- **Validate domain hierarchy**
- **View domain relationships**
- **View a list of tables using domain separation**

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.

**Displaying the domain picker 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>domain_select</td>
<td>Enables the domain selector</td>
</tr>
<tr>
<td>domain_reference_picker</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.

1. Open the System Properties (sys_properties) table.
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-Ul16 interface. Starting with Ul16, 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.

**Validate domain hierarchy**

By default, the instance validates the domain hierarchy every time you change the domain table, change the query method, or reset the records to the global domain.

Role required: admin

Domain hierarchy validation might take an excessive amount of time if there are a large number of records in a table.

The **Domain Progress Workers** list displays any currently running domain tasks. Use the following procedure to manually start the validation process.

---

**Note:** Domain paths are used for all customers on Helsinki and later. Domain numbering is no longer used. ServiceNow Technical Support can assist in the upgrade. When you create a domain or update the parent of a domain, the system runs a scheduled job to recalculate domain paths. The result of the scheduled job, use the following URL: https://<your-instance-name>/syslog_domain_list.do

---

1. Navigate to **Domain Admin > Configuration**.
2. Click **Validate domains hierarchy**.
3. After the validation process completes, review the **Domain Alerts** section for any renumbering or path conversion errors.

The domain validation process automatically fixes some validation errors and provides information about errors that cannot be automatically fixed.
If domain hierarchy validation takes an excessive amount of time due to a large number of records in a table, you can exclude these tables from the validation process. To do so,

1. Add this property to the System Properties (sys_properties) table: glide.sys.domain.validation_skip_threshold.

2. Set the integer value to the maximum number of records that a table can have for it to be validated. Tables with a larger number of records than this value are not validated. The default value is 10000000.

You can also view the domain log by click a domain log record.
<table>
<thead>
<tr>
<th>Created</th>
<th>Level</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014-02-25 12:29:36</td>
<td>Error</td>
<td>2 records detected in 'mytable' that have the same value for the key 'sys_id'.</td>
</tr>
<tr>
<td>2014-02-25 12:29:35</td>
<td>Error</td>
<td>Entries causing the error are as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sys_id:e8f6b726c303110059d85b</td>
</tr>
<tr>
<td>2014-02-25 12:23:56</td>
<td>Information</td>
<td>Updated table: sys_ui_section for domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updating table sys_user for domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updating table sys_user for domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updating table sys_user for domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updating table sys_user for domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updating table sys_user for domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updating table sys_user for domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updating table sys_user for domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updating table sys_user for domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updating table sys_user for domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updating table sys_user for domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updating table sys_user for domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updating table sys_user for domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updating table sys_user for domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updating table sys_user for domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updating table sys_user for domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updating table sys_user for domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updating table sys_user for domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updating table sys_user for domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updating table sys_user for domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updating table sys_user_for_domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updating table sys_user_group_for_domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updating table sys_user_group_for_domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updating table sys_user_group_for_domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updating table sys_user_group_for_domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updating table sys_user_group_for_domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updating table sys_user_group_for_domain</td>
</tr>
</tbody>
</table>
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.

View a list of tables using domain separation

You can view a list of all domain-separated tables from the Configuration module.

Role required: admin

1. Navigate to Domain Admin > Configuration.
2. Click Show tables with sys_domain field.

Exempt roles from the current record domain

By default, all roles use the domain of the current record when Use the domain of the record being viewed instead of the user's own property is true.

Role required: admin

You can provide a list of roles that ignore this property and always use the user's domain rather than the record's domain. You may want certain roles such as administrators to always work from their own domain rather than use the domain of the record they are viewing.

1. Navigate to Domain Admin > Configuration.
2. For List of roles (comma-separated) that will not trigger the automatic change of domain to the domain of the record that is being viewed, enter a comma-separated list of roles that ignore automatic domain change behaviors.
3. Click Save.

Manually re-enable domain separation

Use the following steps to manually re-enable domain separation if it was previously disabled.

Role required: admin

1. Navigate to Domain Admin > Configuration.
2. Select the domain table. For example, to navigate to the Group [sys_user_group] table, click User Administration > Groups.
3. Select the domain query method. For example, Switch to Domain Paths.
4. For Enable domain separation, select the Yes check box.
5. Click Save.

© 2019 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.
Delegated administration

Delegated 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 delegated administration

By default, delegated 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, delegated administration uses the policies for the global domain.

For example, Fred Luddy is a user in the Database domain who can see records in the Database: Atlanta, Database: San Diego, and NY DB child domains. When he opens a record in the Database: San Diego domain, delegated administration first checks for policies in the Database: San Diego domain. If there are no policies at this level of the domain hierarchy, delegated
administration checks for policies from the Database domain. If there are no policies in the Database domain, delegated administration uses the global domain policies as there are no other domains higher in the domain hierarchy.

**Example delegated administration with domain specific applications**

The following example illustrates delegated administration with domain-specific applications and modules.

As the administrator of the Database domain, David Loo decides to customize the Configuration application. To start with, David reviews the modules available in the Configuration application module.

![Application](image1)

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>New Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Management</td>
<td>true</td>
<td>900</td>
<td>asset</td>
<td></td>
</tr>
<tr>
<td>BSM Map</td>
<td>true</td>
<td></td>
<td>admin, itil</td>
<td></td>
</tr>
<tr>
<td>Change</td>
<td>true</td>
<td>400</td>
<td>itil</td>
<td></td>
</tr>
<tr>
<td><strong>CMDB</strong></td>
<td>true</td>
<td>600</td>
<td><strong>inventory_admin</strong></td>
<td></td>
</tr>
<tr>
<td>Content Management</td>
<td>true</td>
<td></td>
<td>content_admin</td>
<td></td>
</tr>
<tr>
<td>Contract Management</td>
<td>true</td>
<td>1,000</td>
<td>asset, contract_manager</td>
<td></td>
</tr>
<tr>
<td>Domain Admin</td>
<td>true</td>
<td></td>
<td>domain_admin</td>
<td></td>
</tr>
<tr>
<td>ECC</td>
<td>true</td>
<td></td>
<td>admin</td>
<td>ecc</td>
</tr>
<tr>
<td>Homepage Admin</td>
<td>true</td>
<td></td>
<td>admin</td>
<td>home</td>
</tr>
<tr>
<td>Incident</td>
<td>true</td>
<td>200</td>
<td>itil</td>
<td>incident</td>
</tr>
<tr>
<td>Instance Clone</td>
<td>true</td>
<td></td>
<td>clone_admin</td>
<td>instance</td>
</tr>
<tr>
<td>Knowledge Base</td>
<td>true</td>
<td>800</td>
<td>knowledge</td>
<td>km</td>
</tr>
<tr>
<td>Metrics</td>
<td>true</td>
<td></td>
<td>itil_admin, metric_admin</td>
<td></td>
</tr>
<tr>
<td>MID Server</td>
<td>true</td>
<td></td>
<td>admin</td>
<td>MID</td>
</tr>
<tr>
<td>Organization Management</td>
<td>true</td>
<td>875</td>
<td>asset</td>
<td>organization</td>
</tr>
<tr>
<td>Problem</td>
<td>true</td>
<td>300</td>
<td>itil</td>
<td>problem</td>
</tr>
<tr>
<td>Reports</td>
<td>true</td>
<td>1,100</td>
<td>itil</td>
<td>report</td>
</tr>
<tr>
<td>SAML 2 Single Sign-on</td>
<td>true</td>
<td></td>
<td>admin</td>
<td>saml</td>
</tr>
<tr>
<td>SAML Single Sign-on</td>
<td>true</td>
<td></td>
<td>admin</td>
<td></td>
</tr>
</tbody>
</table>

© 2019 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 Database category.

This creates a new module entry in the application rather than overwriting the existing module in the global domain.
<table>
<thead>
<tr>
<th>Title</th>
<th>Table</th>
<th>Active</th>
<th>Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create New</td>
<td>incident</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>Assigned to me</td>
<td>incident</td>
<td>true</td>
<td>active=true</td>
</tr>
<tr>
<td>Open</td>
<td>incident</td>
<td>true</td>
<td>active=true</td>
</tr>
<tr>
<td>Open - in &quot;New&quot; state</td>
<td>incident</td>
<td>true</td>
<td>incident_state</td>
</tr>
<tr>
<td>Open - Unassigned</td>
<td>incident</td>
<td>true</td>
<td>assigned_to</td>
</tr>
<tr>
<td>Resolved</td>
<td>incident</td>
<td>true</td>
<td>state=6^EQ</td>
</tr>
<tr>
<td>Closed</td>
<td>incident</td>
<td>true</td>
<td>active=false</td>
</tr>
<tr>
<td>All</td>
<td>incident</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>Overview</td>
<td></td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>Critical Incidents Map</td>
<td></td>
<td>true</td>
<td></td>
</tr>
</tbody>
</table>

Update  Delete

© 2019 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.
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.
Example delegated administration with domain specific policies

The following example illustrates delegated administration with domain-specific policies. In this hierarchy, David Loo is in the Database domain and Don Goodliffe is in the Database/Database San Diego domain.

To begin, David Loo makes a change to the global assignment policy. Then Don Goodliffe also makes a change to the same policy. Initially, all assignment rules have a global domain as shown below:
Global domain rules

If David Loo updates the assignment rule for **Database or Software**, the following list appears:

Database domain-specific rules

The following policy changes occur:
When the policy is chosen and updated, the system detects that David Loo is not at the right level of the hierarchy to change this record. Therefore, the update is changed into an insert, and a new record is created.

The new policy has the same name (Database or Software).

Notice that this policy is in the Database domain and overrides the policy that previously applied (Database or Software). Notice that there are now two policy entries with the same name. Because this is not desirable, David opens the record and changes the name to something appropriate. After the update, the list appears as follows.

Renamed database or software to database specific policy

This time, the record being updated is at the same level in the domain hierarchy as the user, so the record is updated with a more appropriate name. Here is the resulting rule. Notice that database incidents are directly assigned to David.
Database specific policy assignment rule

If a new incident is created in the Database domain or lower in the hierarchy, the new rule is applied. It has overridden the global assignment rule. If a new incident is created in the global domain or any other domain not within the Database domain hierarchy, then the global rule applies.
In the following scenario, Don Goodliffe, in the Database/Database San Diego domain hierarchy, decides that database incidents created in his domain should be assigned to him rather than to David Loo. As an administrator, Don Goodliffe starts out with the following assignment policy:

![Assignment Rules](image)

Don Goodliffe's starting view of assignment rules

Notice that this level of the hierarchy starts out with the policy established at the parent level (the Database domain). After changing the **Database-Specific Policy**, the list looks like this:
Database San Diego rules override Database-specific policy rules

Again, the attempted update is changed automatically to an insert, and the override value is supplied to indicate that the higher-level policy is being overridden. Here is the resulting rule; it shows that database incidents created in the Database San Diego domain are assigned to Don Goodliffe.
San Diego specific policy

The result of the above customization is:

- A database incident from the Database San Diego domain is assigned to Don Goodliffe.
- A database incident from the Database hierarchy other than Database San Diego is assigned to David Loo.
• A database incident from any other domain, including global, is assigned to the system administrator.

The above customizations all show changes to higher-level policy. However, new policy can also be created at any level of the domain hierarchy.

During a transaction, the current user’s domain normally determines the policy to load. For example when a user in the Database domain updates an incident, the Database domain is used for business rules and policies even if the incident record was originally created in the Database San Diego domain. By default, the user’s domain supersedes the record’s domain.

There is a system setting that can change this behavior. If Using the Current Record’s Domain Instead of the Current User’s Domain is set to true, then the above behavior is reversed. The domain of the record is used to determine which policy to load, not the domain of the user. For example if a user in the Database domain updates an incident that is in the Database San Diego domain, then the business rules and policy that exist for Database San Diego are executed. The domain of the user still determines the records that are visible to the user, and the domain of the user sets the domain for records that user creates, but is not a factor in determining rules and policies.

Manually re-enable delegated administration

Delegated administration allows administrators in lower portions of the domain hierarchy to add domain-specific policies that override policies set higher in the domain hierarchy.

Role required: admin

By default, activating domain separation enables delegated administration. Use the following steps to manually re-enable delegated administration if it was previously disabled.

1. Navigate to Domain Admin > Configuration.
2. For Enable delegated administration, select the Yes check box.
3. Click Save.

Enable verbose domain logging and debug messages

Domain log and debug messages allow you to troubleshoot domain configuration errors.

Role required: admin

1. Navigate to Domain Admin > Configuration.
2. For Enable verbose domain logging, select the Yes check box.
3. Click Save.

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.
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 Spool] Query against table incident restricted by
domain values [Database Atlanta[db53580b0a0a0a6501aa37c294a2ba6b],
Database[287ee6fe9f1000ada7950d0b1b73],
Database San Diego[db53a9290a0a650091abebeccf833c6], global, NY
DB[5f74727dc0a8010e01efe33a251993f9]]
```

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.
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.
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:

   Query against table incident restricted by domain values [global,
   Software[8a4dde73c6112278017a6a4ba547aa7]]

   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 sys_domain column value whose sys_id does not exist in the current domain table. The domain sys_id 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 sys_domain value. Then, either manually enter the correct sys_domain value or remove it.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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.</td>
</tr>
<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, validate the domain tree and let the background conversion process run to completion. If the error persists, you can manually edit the value for the sys_domain_path or sys_domain_number 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>

**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.

**Encryption Support**

Use encryption contexts to allow or deny access to sensitive data based on user role.

Encryption and decryption occur on the server, not in the user interface.

**Encryption methods**

Fields that use Encryption Support may include:

- New or existing Encrypted Text fields.
• String and 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>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>
<tr>
<td>Access level</td>
<td>Data access to a field using the single encryption context method</td>
<td>Data access to a field using the multiple encryption contexts method</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------</td>
<td>---------------------------------------------------------------</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 displays 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 displays 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. |
| User with two or more encryption contexts | 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 displays 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 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.  
- **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. | The user can select an encryption context from the encryption context selector in the welcome bar.  
- **If there is no data in the field**: The form displays 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.  
- **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. |

### 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:

© 2019 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.
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.
- (is empty) and (is not empty) returns 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 are displayed 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 Definition > Plugins**.
2. Find and click the plugin name.
3. On the System Plugin form, review the plugin details and then click the **Activate/Upgrade** related link.
   
   If the plugin depends on other plugins, these plugins are listed along with their activation status.
   
   If the plugin has optional features that depend on other plugins, those plugins are listed under **Some files will not be loaded because these plugins are inactive**. The optional features are not installed until the listed plugins are installed (before or after the installation of the current plugin).
4. Optional: If available, 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 practice when you first activate the plugin on a development or test instance.
   
   You can also load demo data after the plugin is activated by clicking the **Load Demo Data Only** related link on the System Plugin form.
5. Click **Activate**.
Set up encryption contexts

Administrators can 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.

<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 this field blank to randomly generate a key. 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**. |
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

The encryption context selector enables users who have 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. In the General tab, select the Show encryption 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.

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.

### Add an Encrypted Text field to a table

Add an Encrypted Text field to a table to create a new encrypted field. Alternatively, you can encrypt existing URL and String fields by changing the field type to Encrypted Text. Encrypted Text fields are installed with the Encryption Support plugin.

Role required: security_admin

1. Open the table.
2. Right-click the header menu and select **Configure > Table**.
3. Add a table column and set the Type to **Encrypted Text**.
4. Save the form.

**Encrypt an existing field**

Create an encrypted field configuration to encrypt the value of an existing String or URL field using Encryption Support.

Role required: **security_admin**

Encrypted field configurations created to encrypt other field types can be deleted. 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 manually create encrypted field configurations to encrypt existing String 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>Column</td>
<td>The field to be encrypted. Only string and URL fields are supported.</td>
</tr>
</tbody>
</table>
| Method         | - **Single Encryption Context**: Enables data to be encrypted with a single encryption context only. The field is encrypted with the encryption context defined in the **Encryption context** field. Users that do not have the encryption context cannot view or update field values.  
- **Multiple Encryption Contexts**: 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.  

**Note**: Mass encryption is not available when using the **Multiple Encryption Contexts** method.  

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.

| Encryption context | The encryption context for the encrypted data. Only visible when **Single Encryption Context** is selected in the **Method** field.  
Once an encrypted field configuration is applied to a field using the single encryption context method, you cannot change the encryption context.  

**Note**: To change an encryption context of an encrypted field configuration, run a mass decryption to decrypt the data, delete the existing encryption configuration, then create a new encryption configuration.
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

Mass encryption is only available when an encrypted field configuration uses the single encryption context method. Mass decryption is available for both the single and multiple encryption context methods. Before deleting an encrypted field configuration, run a mass decryption to decrypt previously encrypted values.

Role required: security_admin

Mass encryption and decryption depend on the encryption contexts available to the user performing the operation.

<table>
<thead>
<tr>
<th>Encryption method</th>
<th>Available actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the field uses the single encryption context method</td>
<td>You must have access to the encryption context defined in the encrypted field configuration record. If you do not have access to the encryption context, the related links in the encrypted field configuration do not display.</td>
</tr>
<tr>
<td>If the field uses the multiple encryption contexts method</td>
<td>During mass decryption, only records encrypted with encryption contexts you have access to are decrypted. If running a mass decryption before deleting an encrypted field configuration, make sure to decrypt all records. This may require multiple security_admin users with access to different contexts or a single security_admin user with access to all relevant encryption contexts to run a mass decryption on a field.</td>
</tr>
</tbody>
</table>

**Note:** It is advised to only run mass encryption and decryption during non-peak hours as 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.
   - Run mass decryption
   - Run mass encryption

   **Note:** Mass encryption is only available if the encryption method is **Single Encryption Context**.

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.
Encrypt an attachment

You can encrypt attachments that are already attached to records.

1. Log in as a user with at least one encryption context.
2. Navigate to a form which 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.
   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.

Encrypt a password in system properties

The Encrypt SysProperty Password business rule automatically encrypts the value of any system property with the type password or password2.

The business rule encrypts passwords when you add a new value or update an existing one. After encrypting the password, the instance always stores and displays the encrypted password value. The instance only decrypts the password in memory and never saves a clear-text version.

After upgrading from an earlier version, encrypt existing properties that contain passwords by updating the value.

1. In the Type filter text, enter sys_properties.list.
2. Select the system property you want to encrypt.
3. Enter or update the Value to change the password.
4. Click **Update**.

   The business rule encrypts the password.
Domain separation in Encryption Support

Encryption Support 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 then control several aspects of this separation, including which users can see and access data.

Overview

Support: Data only

Domain separation in this application is supported at the Data only level, meaning it supports the data security model of separating visibility of data from one domain to another. To learn more, 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.
- Level 1 domain separation is not supported because it would allow Managed Service Providers (MSPs) to create and manage domain-specific encryption contexts and encryption keys across all domains.
- Level 2 domain separation does not apply to encryption.
- Level 3 domain separation is not supported because it would allow domain administrators to create and manage domain-specific encryption contexts and keys for their domain.
Encryption scripting examples

These example scripts show you how to accomplish common encryption tasks.

Encrypt unencrypted attachments

The following sample script encrypts unencrypted attachments, such as in the incident table.

**Note:** Impersonation does not change the encryption contexts available to a user. Even while impersonating, you have only the encryption contexts available to you originally.

```javascript
bulkEncryption();

function bulkEncryption() {
    gs.log("*********** BULK ENCRYPTION RUN BY " + gs.getUserName());
    encryptAttachments("incident", "testContext");
    gs.log("*********** BULK ENCRYPTION COMPLETED");
}

// Note that whomever runs this script must have access to use the
// specified encryption context or nothing will happen when
// "changeEncryptionContext" is called except that a warning will appear
// in the log: WARNING *** WARNING *** Attempt to get
// cipher for encryption context 'contextName' without authorization
function encryptAttachments(table, encryptionContextName) {
    var contextGR = new GlideRecord("sys_encryption_context");
    contextGR.addQuery("name", encryptionContextName);
    contextGR.query();
    if (!contextGR.next()) {
        gs.log("*********** No such encryption context " + encryptionContextName);
        return 0;
    }

    var encryptionId = contextGR.getUniqueValue();

    gs.log("*********** BEGIN ENCRYPTING ATTACHMENTS FOR " + table + " TABLE");
    var attachmentGR = new GlideRecord("sys_attachment");
    attachmentGR.addQuery("table_name", table); // only attachments for the
    specified table
    attachmentGR.addNullQuery("encryption_context"); // only attachments not
    yet encrypted
    attachmentGR.query();
    var count = 0;
    while (attachmentGR.next()) {
        var sysAttachment = new GlideSysAttachment();
        sysAttachment.changeEncryptionContext(attachmentGR.getValue("table_name"),
            attachmentGR.getValue("table_sys_id"),
            attachmentGR.sys_id, encryptionId);
        gs.log("*********** ENCRYPTED [" + attachmentGR.sys_id + "] " +
            attachmentGR.getValue("file_name");
        count++;
    }
    gs.log("*********** ENCRYPTED " + count + " ATTACHMENTS FOR " + table + " TABLE");
    return count;
}
```

To write a script changing the encryption context from one context to another, access to both contexts is required.
Set the encryption context ID

The function `setContextID` is provided to set the encryption context ID of an encrypted field in script.

The argument to the function is the `sys_id` of the encryption context you wish to use. The following example creates records with an encrypted field, `u_subspecies`, encrypted by the “Species Security” encryption context.

**Note:** The user who runs this script must have access to the encryption context.

```javascript
function encrypt() {
    var encryptionID = getEncryptionID("Species Security");
    if (encryptionID == "")
        return;

    createEncryptedRecord("Sumatran tiger", "Panthera", "tigris", "sumatrae", encryptionID);
    createEncryptedRecord("Bengal tiger", "Panthera", "tigris", "tigris", encryptionID);
    createEncryptedRecord("Siberian tiger", "Panthera", "tigris", "altaica", encryptionID);
}

function getEncryptionID(encryptionName) {
    var contextGR = new GlideRecord("sys_encryption_context");
    contextGR.addQuery("name", encryptionName);
    contextGR.query();
    if (!contextGR.next()) {
        gs.log("*********** No such encryption context " + encryptionContextName);
        return "";
    }
    return contextGR.getUniqueValue();
}

function createEncryptedRecord(commonName, genus, species, subspecies, encryptionID) {
    var newRecord = new GlideRecord("u_species_encrypted");
    newRecord.u_common_name = commonName;
    newRecord.u_genus = genus;
    newRecord.u_species = species;

    // We have one encrypted field, u_subspecies.
    newRecord.u_subspecies.setDisplayValue(subspecies);
    newRecord.u_subspecies.setContextID(encryptionID); // use our encryption context for the field
    newRecord.insert();
}
```

Remove encryption contexts

These functions remove an encryption context, or all encryption contexts, from those available to the user session.
This can be used by customers in a script to further limit the encryption contexts that are available to a user under certain conditions. For example, a synchronous Script Action triggered by the `session.established` event could remove all encryption contexts if a user was not connecting from an IP in a certain range.

```java
if (some condition) {
    var contexts = gs.getSession().getEncryptionContext();
    contexts.removeAllContexts();
}
```

Individual encryption contexts can be removed as well using the `sys_id` of the encryption context.

```java
if (some condition) {
    var contexts = gs.getSession().getEncryptionContext();
    contexts.removeContext("077d9b3307211000e2bb5720e1021e61");
}
```

**Return a decrypted field value**

You can return the field value for an encrypted field by using the `getDisplayValue` method.

**Demonstration plugin**

The instance provides a demonstration plugin called Encryption Support - Single Context Task Encryption Demo (com.snc.task_encryption.demo).

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.
**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
- Edge Encryption release notes
- Understanding Edge Encryption
- Edge Encryption components
- Encryption configurations and patterns
- Domain separation in Edge Encryption

### Set up
- Planning for Edge Encryption
- Edge Encryption system requirements
- Edge Encryption installation
- Edge Encryption upgrades

### Administer
- Key management
- Encrypt fields using encryption configurations
- Encrypt attachments using standard encryption
- Tokenize strings using encryption patterns

### Use
- Define a custom encryption rule
- Schedule an encryption job
- Repair or recover order-preserved encrypted data

### Integrate
- Edge Encryption ODBC driver integration
- Edge Encryption MID Server integration

### Troubleshoot and get help
- Ask or answer questions in the Edge Encryption forum
- Edge Encryption diagnostics and performance
- Search the HI knowledge base for known error articles
- Contact ServiceNow Technical Support

---

**Understanding Edge Encryption**

Edge Encryption is a network encryption system that resides in your network that encrypts and decrypts sensitive data as it travels between your data center and the ServiceNow cloud.

**What is Edge Encryption**

The Edge Encryption proxy server is a network encryption application that, through encryption in motion, encrypts data within your network before it is sent over the Internet to your instance, where it remains encrypted at rest. When requested, the encrypted data is sent back to the Edge Encryption proxy server, which in turn decrypts your data before serving it to your web browser.

**Who uses Edge Encryption**

Encrypted data can only be viewed in clear text by a user logged in to the instance through a proxy server in your network. Likewise, Edge Encryption can only be configured and administered by a security_admin user logged in to an instance through a proxy server in your network.

Because the proxy server resides in your network, you own and manage the encryption keys—they are never sent to the instance. As a result, sensitive data is never displayed in clear text to ServiceNow.
Edge Encryption can encrypt or tokenize your data

Edge Encryption supports both encryption and tokenization as a means of protecting your sensitive information.

Encryption configurations

You can encrypt individual fields using encryption configurations. Edge Encryption supports AES with 128-bit and 256-bit encryption keys. Standard, equality-preserving, and order-preserving encryption types are supported.

In addition to attachments, the following field types can be encrypted:

- String
- 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.

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 by reviewing Planning for Edge Encryption.
What to know before you begin

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.

- Edge Encryption system requirements
- Sizing your Edge Encryption environment
- Edge Encryption limitations
- Key management

Learn more

This podcast offers more information about 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>
</tbody>
</table>
### Backing 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.

### Key management

You are responsible for providing and managing the encryption keys used by Edge Encryption. 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 store, 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**

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.

**Important:** Edge proxies installed before this release support SafeNet keys, but do not support SafeNet key versioning. If you mistakenly use a versioned key on an older proxy, when you upgrade to the London release, the London 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 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 with 128-bit encryption keys. If the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy files are installed, Edge Encryption supports 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>
<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>

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**

Edge Encryption adds the following tables.

<table>
<thead>
<tr>
<th>Table Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edge Encryption Configuration (sys_encryption_configuration)</td>
<td>Contains encrypted fields and tables for which attachments are encrypted.</td>
</tr>
<tr>
<td>Edge Encryption Rule (sys_encryption_rule)</td>
<td>Contains a record for each rule. A rule has a name, the condition when it is used, a script, and an order field.</td>
</tr>
<tr>
<td>Edge Encryption Invalid Insert Log (sys_edge_encryption_invalid_insert_log)</td>
<td>Contains log messages created for attempts to save unencrypted data to an encrypted field.</td>
</tr>
<tr>
<td>Edge Encryption Proxy (sys_encryption_proxy)</td>
<td>Contains information about the encryption proxy application.</td>
</tr>
<tr>
<td>Edge Proxy Encryption Type (sys_proxy_encryption_type)</td>
<td>Used for enabling and disabling encryption types on the encryption form.</td>
</tr>
<tr>
<td>Encryption Job Execution (sys_encryption_job_execution)</td>
<td>Supports mass encryption jobs.</td>
</tr>
<tr>
<td>Encryption Job Execution Chunk (sys_encryption_job_execution_chunk)</td>
<td>Supports mass encryption jobs.</td>
</tr>
<tr>
<td>Scheduled Encryption Job (sysauto_encryption_job)</td>
<td>Lists scheduled jobs for encryption, decryption, key rotation, order token repair, and database recovery.</td>
</tr>
<tr>
<td>Encryption Key Configuration (sys_encryption_key_configuration)</td>
<td>Lists default encryption keys.</td>
</tr>
<tr>
<td>Encryption Key (sys_encryption_key)</td>
<td>Lists available keys and key attributes.</td>
</tr>
<tr>
<td>Proxy Encryption Key (sys_encryption_proxy_key)</td>
<td>Lists proxy encryption keys.</td>
</tr>
</tbody>
</table>

**Properties**

Edge Encryption adds the following properties.
**Properties for Edge Encryption**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 |
Roles installed with Edge Encryption

<table>
<thead>
<tr>
<th>Role title</th>
<th>Description</th>
<th>Contains roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>edge_encryption</td>
<td>Edge Encryption proxies log into the instance as a user, with a user name and password. The user must have this role assigned.</td>
<td>None</td>
</tr>
</tbody>
</table>

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.
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.

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 &lt;Java-home-directory&gt;/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 earlier.</td>
</tr>
</tbody>
</table>
Java Version | Enabling AES 256-bit Encryption
--- | ---
Java 8 update 151 (8u151) or later | A `java.security` file is downloaded with the update. You can simply edit the `java.security` file to enable AES 256-bit encryption. See [Enable AES 256-bit encryption for Java 8 update 151 (8u151) or later](#).

**Note:** 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.

---

**Note:** Java does not automatically allow unlimited strength keys. You must specifically enable the use of AES 256-bit encryption.

---

**Proxy server minimum configuration**

A proxy server requires this minimum configuration:

- 4 GB of available 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 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 considerations.
- Ability to run concurrently with other services, depending on the server utilization and resource availability.
- Java 8.

**Proxy server supported systems**

The following systems are supported:

<table>
<thead>
<tr>
<th>Supported System</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2012, 2012-R2, and 2016 editions</td>
<td>• Virtual machines or physical hardware&lt;br&gt;• 64-bit systems</td>
</tr>
</tbody>
</table>
Supported System | Description
--- | ---
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:

```bash
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>MySQL Database</td>
<td>Requirement</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</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 record size. See Calculate the order-preserving and tokenization database size.</td>
</tr>
<tr>
<td>Configuration</td>
<td>High availability cluster. If you are unsure of how to configure your MySQL server, contact MySQL for configuration information.</td>
</tr>
</tbody>
</table>

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.

| Note: 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**

Restrictions on encrypting field types.

- The following field types can be encrypted:
  - String
  - Journal
  - Journal Input
  - URL
Choice fields, virtual fields, and any fields other than String and Journal fields cannot be encrypted. See Field types for more information.

- Fields in system tables, except for certain fields in sys_user, cannot be encrypted.
- System fields in tables cannot be encrypted.
- Fields named "number" and fields associated with an auto-numbering scheme cannot be encrypted.
- 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, only order preserving and equality preserving encryption types can be used. Indexed fields cannot be encrypted using the standard encryption type.

Configuration restrictions

Restrictions and behavior of encryption configurations.

- After a field has been added to the Edge Encryption Configuration table, the configuration record cannot be deleted. 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 in all inherited tables is also encrypted. 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 the 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. Importing data to a field with an encryption configuration defined is not supported.

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 encryption will still pass equivalence checks when compared against an identical encrypted value.

- 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.
- Other than file store, Java KeyStore, SafeNet, and Unbound Technology, no third-party software or hardware encryption key management is supported.
While 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 values included in emails are encrypted.

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.

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.

**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><code>edgeencryption.proxy.host</code></td>
<td>hostname.mycompany.com</td>
</tr>
<tr>
<td><code>edgeencryption.proxy.http.port</code></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 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: none

1. In the HI Service Portal, click **Service Requests > Activate Plugin**.
2. Fill out the form.

<table>
<thead>
<tr>
<th>Target Instance</th>
<th>Instance on which to activate the plugin.</th>
</tr>
</thead>
<tbody>
<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>Date and time must be at least 2 business days from the current time.</td>
</tr>
</tbody>
</table>

**Note:** Plugins are activated in two batches each business day in the Pacific time zone, once in the morning and once in the evening. If the plugin must be activated at a specific time, enter the request in the Reason/Comments.
3. 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.

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:** As 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 London 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 using the interactive installer

Install the Edge Encryption proxy server on a Windows or Linux computer using the interactive installer.

**Important:** 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 <strong>Detect FQDN</strong> 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.

**Important:** 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 JavaPasswordSDK.jar file installed on the host Windows machine during CyberArk configuration.</td>
</tr>
<tr>
<td>App ID</td>
<td>The <strong>App ID</strong> entered during CyberArk configuration.</td>
</tr>
<tr>
<td>Safe Name</td>
<td>The <strong>Safe Name</strong> 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>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</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.
   - The key alias is the given alias for the 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. Use the 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.

1. **Select the location to store the encryption key.**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>File Store</strong></td>
<td>Use a file to store a single encryption key. You can use an existing file in the <code>/keys</code> 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>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><strong>Java KeyStore File</strong></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><strong>New Key</strong></td>
<td>Create an encryption key and alias. The alias name (key name, key alias) must use lowercase letters and numbers, per Java KeyStore requirements. To find out more about the keytool utility, see the <strong>Java SE Documentation</strong>.</td>
</tr>
<tr>
<td><strong>Use Existing Key</strong></td>
<td>Use an existing encryption key in the selected keystore.</td>
</tr>
<tr>
<td><strong>Import Existing Key</strong></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.
Default Encryption Key

This step requires you to go to your instance and create a default key. Click the links below and follow the instructions. Click 'Next' when you are done setting up the default key on your instance.

The 'Key alias' must be: aes128
The 'Key size' must be: 128
The 'Type' must be: Keystore

Click here for documentation
Click here to go to your default keys

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 Encryption 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.

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. Use an existing file in the /keys directory or 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>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. Optional: If you want to use AES 256-bit encryption, do the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Choice</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. Once the key is configured on the instance, return to the installer and click **Next**.

**Configure the Edge Encryption proxy database**

If using order-preserving encryption types or encryption patterns, 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.
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.
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>Option</td>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</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>-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>

**Caution:** 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 (e.g. 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`.

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>
</tbody>
</table>
### 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you have a PKCS12 (.pfx) file that contains the RSA key and the certificate.</td>
<td>keytool -importkeystore -destkeystore keystore.jceks -deststoretype jceks -srckeystore &lt;PKCS12 filename&gt; -srckeystore 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

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.

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 machine, 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 machine 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 machine, where JRE_HOME is an environment variable for both 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 keystore and encryption keys

Set up the keystore and encryption keys used by the Edge Encryption proxy server.

1. Carefully determine the appropriate type of keystore to use based on your organization's needs.

<table>
<thead>
<tr>
<th>Supported keystore</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>
</tbody>
</table>
| **Java KeyStore**  | A Java KeyStore:
• Stores keys in a Java JCEKS KeyStore.
• Is password protected and more secure than storing keys in a file in the file system.
• Can store multiple keys. A key alias represents each key, making it easier to manage multiple keys. 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. |
Supported keystore | Description
---|---
Enterprise Key Management (EKM) | **SafeNet KeySecure**

Keys are stored and retrieved with SafeNet KeySecure key management.

You must secure a license with [Gemalto](https://www.gemalto.com), 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.

**Unbound Technology**

The base64-encoded wrapped encryption key is stored as a text file on the Edge Encryption proxy server. The Unbound Technology implementation (previously Dyadic Security) maintains control of the wrapping key.

The Edge Encryption proxy server must run on the same machine as the Unbound technology client.

**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, 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.

   Note: If you choose to run these commands from a directory other than the keystore directory, that is you skipped the previous step, you must change the -keystore option to include the path from your current directory to the keystore directory. For example, if you were in the <installation directory>/bin directory, the option would be -keystore ../keystore/keystore.jceks

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES 128</td>
<td>keytool -genseckey -alias 128bitkey -keyalg aes -keysize 128 -keystore keystore.jceks -storetype jceks</td>
</tr>
<tr>
<td>AES 256</td>
<td>keytool -genseckey -alias 256bitkey -keyalg aes -keysize 256 -keystore keystore.jceks -storetype jceks</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 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/OAEPWITHSHA-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) Change to the `<proxy-installation-directory>/conf` directory.
   b) Open the `edgeencryption.properties` file.
   c) 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.
      For more information on Edge Encryption properties, see [Edge Encryption proxy server properties](#).
   d) 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.
   e) 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.

This step creates both the key storage and the 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 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.

   Note: If using SafeNet versioned keys, an additional column appears for the Key version. The Key version cannot be edited.

   Important: If using SafeNet versioned keys, click the Retrieve latest key versions link in the Related Links to retrieve the latest version of each key from the Edge proxy.

   Rows in the list with an X in the left column can be deleted. Keys that have been used as the default or that have a Status of Available cannot be deleted.

   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.

      Key aliases are lowercase letters and numbers. Capital letters are changed to lowercase letters when you click Update. Key aliases must be unique.

      Note: If using Unbound technology keys, add the encryption key alias. 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.

   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.

      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.

   Note: If using SafeNet versioned keys, an additional column appears for the Key version. The Key version cannot be edited.

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.
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.

**Configure a web proxy**

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:

```
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:

```
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**

```
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.

**Note:** The first time you set up the `edgeencryption.properties` file or change properties, you may not want to set the password encryption property. After you have verified that everything is working, you can set the password encryption property, shut down the proxy, and then restart the proxy.

1. Run the proxy server.
### Option Description

<table>
<thead>
<tr>
<th>On a Linux machine</th>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1.</td>
<td>cd to ServerName_port</td>
</tr>
<tr>
<td></td>
<td>2.</td>
<td>Execute ./startup.sh</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>On a Windows machine</th>
<th>Perform the following steps from the command line as admin:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. cd to ServerName_port/bin</td>
</tr>
<tr>
<td></td>
<td>2. 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>edgeencryption.proxy.name</td>
<td>Unique name of the proxy server</td>
</tr>
<tr>
<td>edgeencryption.proxy.host</td>
<td>The server name, IP address, or fully-qualified domain name of the computer running the proxy.</td>
</tr>
<tr>
<td>edgeencryption.proxy.http.port</td>
<td>Port on the proxy for HTTP communication. Must be unique across all processes on the machine.</td>
</tr>
<tr>
<td>edgeencryption.proxy.https.port</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.

**Caution:** You must perform this step before launching the proxy server.

<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</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*.

### 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></td>
</tr>
<tr>
<td></td>
<td>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);
    }
```

© 2019 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.
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.
### Target (instance) properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>edgeencryption.target.host</td>
<td>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.servicenow.com</td>
</tr>
<tr>
<td>edgeencryption.target.port</td>
<td>Instance port. Must be the same for all encryption proxies connecting to the same instance. This property is set when the proxy is installed.</td>
</tr>
</tbody>
</table>
| 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

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>edgeencryption.target.username</td>
<td>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.</td>
</tr>
<tr>
<td>edgeencryption.target.password</td>
<td>Password that the proxy uses to log in to the instance.</td>
</tr>
</tbody>
</table>

### Proxy properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>edgeencryption.proxy.host</td>
<td>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.</td>
</tr>
<tr>
<td>edgeencryption.proxy.name</td>
<td>Proxy name. Must be unique for each proxy.</td>
</tr>
<tr>
<td>edgeencryption.proxy.http.port</td>
<td>Port on the proxy for HTTP communication.</td>
</tr>
<tr>
<td>edgeencryption.proxy.https.port</td>
<td>Port on the proxy for HTTPS communication.</td>
</tr>
</tbody>
</table>
### SSL certificate properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>edgeencryption.proxy.https.cert.alias</td>
<td>Alias of the certificate provided by the proxy server to connecting clients.</td>
</tr>
<tr>
<td>edgeencryption.proxy.https.keystore.path</td>
<td>Path to the keystore that contains the HTTPS certificate.</td>
</tr>
<tr>
<td>edgeencryption.proxy.https.keystore.password</td>
<td>Password for the keystore that contains the HTTPS certificate.</td>
</tr>
</tbody>
</table>

### Proxy configuration locked property

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>edgeencryption.proxy.locked</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Proxy database properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>edgeencryption.db.url</td>
<td>Proxy database location. Must be the same for all encryption proxies connecting to the same instance.</td>
</tr>
<tr>
<td>edgeencryption.db.user</td>
<td>User name for accessing the proxy database. Must be the same for all encryption proxies connecting to the same instance.</td>
</tr>
<tr>
<td>edgeencryption.db.password</td>
<td>Password to access the proxy database. Must be the same for all encryption proxies connecting to the same instance.</td>
</tr>
<tr>
<td>edgeencryption.db.name</td>
<td>Proxy database name. Must be the same for all encryption proxies connecting to the same instance.</td>
</tr>
<tr>
<td></td>
<td>• Default value: <code>edgeencryption</code></td>
</tr>
<tr>
<td>edgeencryption.db.bootstrap.file</td>
<td>Bootstrap file for the proxy database. The file is relative to the <code>sql/</code> directory. Must be the same for all encryption proxies connecting to the same instance.</td>
</tr>
</tbody>
</table>

**Note:** Under normal circumstances, this parameter should not be changed.
### Digital signature properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>edgeencryption.proxy.signature.keystore.path</td>
<td>Path and Java KeyStore file name.</td>
</tr>
<tr>
<td>edgeencryption.proxy.signature.keystore.password</td>
<td>Password. The default password is <code>&lt;changeme&gt;</code>. Change the password after installing the Java KeyStore.</td>
</tr>
<tr>
<td>edgeencryption.proxy.signature.keystore.keyalias</td>
<td>The key alias given as the <code>-alias</code> argument when the RSA key pair is generated.</td>
</tr>
</tbody>
</table>

### NAE device keystore

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>edgeencryption.nae.retries</td>
<td>Number of retries to make.</td>
</tr>
<tr>
<td>edgeencryption.nae.enabled</td>
<td>Setting indicates whether an NAE device is available.</td>
</tr>
<tr>
<td>edgeencryption.nae.server</td>
<td>Name of the NAE server.</td>
</tr>
<tr>
<td>edgeencryption.nae.port</td>
<td>Port used by the NAE server.</td>
</tr>
<tr>
<td>edgeencryption.nae.protocol</td>
<td>Protocol used by the NAE server.</td>
</tr>
<tr>
<td>edgeencryption.nae.keystore.path</td>
<td>Path to the keystore on the NAE server.</td>
</tr>
<tr>
<td>edgeencryption.nae.keystore.password</td>
<td>NAE keystore password.</td>
</tr>
<tr>
<td>edgeencryption.nae.username</td>
<td>User name to use to authenticate with the NAE device.</td>
</tr>
<tr>
<td>edgeencryption.nae.password</td>
<td>Password to use to authenticate with the NAE device.</td>
</tr>
<tr>
<td>edgeencryption.nae.client.certificate</td>
<td>Certificate located in the keystore on the NAE server. Set this property to authenticate using a certificate instead of a username and password.</td>
</tr>
</tbody>
</table>

### Clear text and static IV properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>edgeencryption.customer.assigned.known.cleartext</td>
<td>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.</td>
</tr>
<tr>
<td>edgeencryption.encrypter.static.iv</td>
<td>Static IV (initialization vector) used in equality-preserving and order-preserving encryption. This property must be the same for all proxies and it must be exactly 16 bytes (16 ASCII characters).</td>
</tr>
</tbody>
</table>
### Password property

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>edgeencryption.encrypter.properties.password</td>
<td>Name of the file in the <code>conf</code> folder that contains a string used within a secure process to obfuscate passwords in the <code>edgeencryption.properties</code> 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.</td>
</tr>
</tbody>
</table>

### Web proxy properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>edgeencryption.webproxy.host</td>
<td>Web proxy name or IP address.</td>
</tr>
<tr>
<td>edgeencryption.webproxy.port</td>
<td>Port on the web proxy.</td>
</tr>
<tr>
<td>edgeencryption.webproxy.user</td>
<td>User name used to connect to the web proxy. If your web proxy does not use authentication, leave this property commented out.</td>
</tr>
<tr>
<td>edgeencryption.webproxy.password</td>
<td>Password to use to connect to the web proxy. If your web proxy does not use authentication, leave this property commented out.</td>
</tr>
</tbody>
</table>

### Java KeyStore properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>edgeencryption.keystore.path</td>
<td>Path to the Java KeyStore. If using a file store or a SafeNet KeySecure keystore, leave this property commented out. Example:</td>
</tr>
<tr>
<td>edgeencryption.keystore.path =</td>
<td><code>keystore/keystore.jceks</code></td>
</tr>
<tr>
<td>edgeencryption.keystore.password</td>
<td>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.</td>
</tr>
</tbody>
</table>
File store properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>edgeencryption.keyfile.directory</td>
<td>The directory specifies where key files are stored.</td>
</tr>
<tr>
<td></td>
<td>If using the Java KeyStore or a SafeNet KeySecure keystore, leave this property commented out.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>edgeencryption.keyfile.directory=keys</td>
</tr>
<tr>
<td></td>
<td>If using Unbound Technology keys, uncomment this property and set the value to the keys directory.</td>
</tr>
</tbody>
</table>

Unbound Technology provider properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>edgeencryption.ekm.provider.classname</td>
<td>Internal class name for the implementation.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Do not change this property.</td>
</tr>
<tr>
<td>edgeencryption.thirdparty.vendor.library.path</td>
<td>Path to the Unbound API JAR file on the Unbound client machine.</td>
</tr>
<tr>
<td>edgeencryption.ekm.provider.rsa.wrapping.key.alias</td>
<td>Wrapping key alias in the Unbound Technology implementation. Must be the same for all proxies.</td>
</tr>
</tbody>
</table>

General configuration properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>edgeencryption.config.poll.interval</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Do not change this property. Changing the default setting of the Proxy Poll Interval can result in detection delays when a proxy comes online.</td>
</tr>
<tr>
<td>edgeencryption.rules.dir</td>
<td>Folder where the encryption rules are stored on the proxy.</td>
</tr>
<tr>
<td>edgeencryption.encryption.order_preserving.cache.size</td>
<td>Maximum cache size, in bytes.</td>
</tr>
<tr>
<td>edgeencryption.jobs.concurrency</td>
<td>Maximum number of mass encryption jobs that can run concurrently on this proxy.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>edgeencryption.jobs.requests_per_second</td>
<td>Number of http job requests per second that can be sent to the instance by this proxy.</td>
</tr>
<tr>
<td>edgeencryption.attachments.request.timeout.seconds</td>
<td>Attachment upload request timeout in seconds.</td>
</tr>
<tr>
<td>edgeencryption.request.buffer.size</td>
<td>Size of an encryption request. If an encryption request is larger than this size, the excess is saved to disk.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Do not change this property.</td>
</tr>
<tr>
<td>edgeencryption.httpclient.request.buffer.size</td>
<td>Size of the client request. If the client request is larger than this size, the excess is saved to disk.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Do not change this property.</td>
</tr>
<tr>
<td>edgeencryption.proxy.idle.timeout</td>
<td>Time in seconds after which a transaction times out. The default value is <strong>300</strong>.</td>
</tr>
<tr>
<td>edgeencryption.proxy.keepalive.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 <strong>10</strong>. The minimum value is <strong>5</strong>.</td>
</tr>
<tr>
<td>edgeencryption.register.retry.count</td>
<td>Maximum number of times the proxy will ping the instance to try to register. The default is <strong>0</strong> (no limit).</td>
</tr>
<tr>
<td>edgeencryption.tokenization.exclusion.list</td>
<td>Encryption patterns cannot tokenize strings found in these fields.</td>
</tr>
</tbody>
</table>

**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*.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>edgeencryption.stat.collection.enabled</td>
<td>Enables the collection of statistics used by the Edge Encryption proxy server performance dashboard.</td>
</tr>
<tr>
<td></td>
<td><strong>Default value:</strong> <strong>true</strong></td>
</tr>
<tr>
<td></td>
<td>Add this property and set the value to false to disable the collection of statistics used by the Edge Encryption proxy server performance dashboard. After adding proxy server performance properties, you must restart the proxy server for the change to take effect.</td>
</tr>
</tbody>
</table>
### ServiceNow London Now Platform Administration

#### Property

**Property**  | **Description**
--- | ---
`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**

After adding proxy server performance properties, you must restart the proxy server for the change to take effect.

---

**Deprecated proxy encryption properties**

**Edge Encryption properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>edgeencryption.encrypter.default.key128</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>edgeencryption.encrypter.default.key256</code></td>
<td>Specifies the name of the current AES 256 key. Must be the same for all proxies.</td>
</tr>
<tr>
<td><code>edgeencryption.encrypter.key</code></td>
<td>Specifies the key name. This property is specified 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.</td>
</tr>
<tr>
<td><code>edgeencryption.encrypter.type</code></td>
<td>Specifies the type of encryption keystore system.</td>
</tr>
<tr>
<td><code>edgeencryption.encrypter.file</code></td>
<td>Specifies the path and file name of the text file associated with the key.</td>
</tr>
<tr>
<td><code>edgeencryption.encrypter.password</code></td>
<td>Specifies the password for accessing the keystore.</td>
</tr>
</tbody>
</table>

---

**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 London release adds properties to 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>
<tbody>
<tr>
<td><code>edgeencryption.proxy_rewrite_location.host</code></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>- If there is a load balancer in the proxy setup, specify the host name used to access ServiceNow through the load balancer.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Optional:</strong> If there is no load balancer in the proxy setup, can be set to the host name used by the proxy server.</td>
</tr>
<tr>
<td><code>edgeencryption.proxy_rewrite_location.https_port</code></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>- If there is a load balancer in the configuration, specify the HTTPS port used to access ServiceNow through the load balancer.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Optional:</strong> If there is no load balancer in the configuration, can be set to the HTTPS port used by the proxy server.</td>
</tr>
</tbody>
</table>

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 blacklist 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.

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.

   **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.

   **Caution:** 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.
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 ServiceNow Technical 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.
Caution: 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.

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 earlier.

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 London release, your environment supports proxy servers from any London 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, see [Enable AES 256-bit encryption for Java 8 update 141 (8u141) or earlier](#).

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.

**Caution:** 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>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td>Status</td>
<td>The status of the upgrade. This value is read-only. Possible statuses include: Pending, Running, Complete, Failed</td>
</tr>
</tbody>
</table>

<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 earlier**.

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>-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.

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 earlier](#).

**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 London 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 \( \text{<proxy name>\_backup} \).

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 job.

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.

---

**Note:** Before removing 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.

**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 <a href="#">Single Key Rotation</a>.</td>
</tr>
<tr>
<td>Key</td>
<td>Enter the key to be retired. Verify that this key is no longer the default key in <a href="#">Edge Encryption Configuration &gt; Encryption Key Configuration &gt; Set Default Keys</a>.</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>
</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.
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 <strong>Attachment Key Rotation</strong>.</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’s 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 hold the extra space needed 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. 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>The table containing 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 table field to be encrypted. This field appears when the <strong>Type</strong> is <strong>Column</strong>.</td>
</tr>
<tr>
<td>Encryption type</td>
<td>The encryption type to use.</td>
</tr>
</tbody>
</table>

**Note:** A specific table and field combination can only have one active configuration at a time.

3. Click Submit.

After the encryption record has been added, you can create an encryption job to encrypt existing data. If you do not run an encryption job, the existing data is encrypted the next time it is changed.

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 Encryption.</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**.
Schedule a decryption job
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.

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 <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. <strong>Note:</strong> The estimate may be larger than the actual number of records processed.</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 open or download the attachments.
  - 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.
3. Under **Related Links,** click **Schedule Mass Encryption 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>Active</td>
<td>Clear this check box if you want to deactivate this job.</td>
</tr>
<tr>
<td>Job Type</td>
<td>Select <strong>Attachment Encryption.</strong></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.
3. Under **Related Links,** click **Schedule Mass Attachment 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>Attachment Decryption.</strong></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>Basic</td>
<td>A series of character types. In the Basic Pattern Input tab, click <strong>Add</strong> and select a character type. The Sample pattern displays the pattern as characters are added. Click <strong>New Block</strong> to move the next character to the next line. This enables you to group characters in a long pattern. Click <strong>X</strong> to delete the last character in the pattern.</td>
</tr>
<tr>
<td>Advanced</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 <strong>Validate</strong> 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.

<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>Order Token Repair</strong>.</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**.

**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 **Estimate Record Count**.

**Blacklist requests from an IP address in your network**

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 blacklist IP addresses, IP ranges, or network masks. Any connection to the proxy server from a blacklisted address is terminated and is not forwarded to your instance.

Role required: security_admin

To blacklist an IP address, you must be logged in to your instance through the proxy server.

**Important:** Ensure that you understand your network topology before blacklisting IP addresses in your network. If an IP address is added to the blacklist, any user with that IP address will be blocked from accessing the Edge Encryption proxy server.

1. Navigate to **Edge Encryption Configuration > Maintenance > Blacklist IP Addresses**.
The Encryption Proxy IP Blacklists (edge_encryption_ip_blacklist) list view opens.

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 blacklisted addresses.</td>
</tr>
<tr>
<td>IP, IP range, or net-mask</td>
<td>Requests from this IP address, range, or network mask are not forwarded to your ServiceNow instance. Example values include:</td>
</tr>
<tr>
<td></td>
<td>• IP address: 10.10.10.5</td>
</tr>
<tr>
<td></td>
<td>• IP range: 10.10.10.1-15</td>
</tr>
<tr>
<td></td>
<td>• Network mask: 10.10.10.0/24</td>
</tr>
<tr>
<td>Active</td>
<td>Whether the record is active. Only IP addresses from active records are prevented from sending requests to the instance.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the blacklist record.</td>
</tr>
</tbody>
</table>

4. Click **Submit**.
5. Repeat these steps for all other proxies for which an IP address should be blacklisted.

The Edge Encryption proxy server terminates any connection from a blacklisted IP addresses, range, or network mask 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>&lt;RecordProducerName&gt;</td>
<td>Rule created to process POST parameters from the Service Catalog and map variables to fields in the instance.</td>
</tr>
<tr>
<td>&lt;RecordProducerName&gt;Json</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.
```javascript
function ReportOutageJsonCondition(request) {
    if (request.path.endsWith('/servicecatalog/items/*')) {
        var res = request.path.split('/');
        var resBody = res[res.length - 1];
        return true;
    }
    return false;
}
```

```javascript
function ReportOutageJsonAction(request) {
    var tableName = 'incident';
    // Some fields are set in script, additional parameter lines may need to be added
    var currentComments = request.currentComments;
    var currentComment = currentComments[0].comment; // currentComment does NOT replace existing values
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShort description;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request.currentPriority;
    var currentStatus = request.currentStatus;
    var currentDescription = request.currentDescription;
    var currentShortDescription = request.currentShortDescription;
    var currentCreatorId = request.currentCreatorId;
    var currentAssigneeId = request.currentAssigneeId;
    var currentPriority = request. 
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>• <strong>Firefox Network Monitor</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Chrome Network Panel</strong></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>• <strong>Wireshark</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>HTTP Scoop</strong></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** box, select an HTTP method.
   - HTTP Post
   - HTTP Get
   - HTTP Put
   - HTTP Patch
   - HTTP Delete

   **Note:** Pre-Jakarta instances only allow **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.
- An XML 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.

```javascript
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:

**Request object fields**

<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>

```javascript
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 XMLContent.</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.

```javascript
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.

```javascript
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.

ParameterValue - toString()
Converts the POST or URL parameter value to a string.

<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.

<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.

<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 content as an iterable <code>XMLContent</code>.</td>
</tr>
</tbody>
</table>
### 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 XMLContent.</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.

<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.

<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.

© 2019 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.
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.

```xml
<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:

```javascript
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.
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');
        } else {
            // if table is not incident, ask the proxy to check if the given field is encrypted for the given table
            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>
    </record>
</data>
```
The following encryption rule action can apply:

```javascript
function sampleXmlAction3() {
    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) {
    // 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.

<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>
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.

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 XMLElement object to start.</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>

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>

### Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>void</td>
<td></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>

### Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>void</td>
<td></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>

### Returns

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>The element name.</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"
    }
}
```
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_description');
    }
}
```

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());
    }
}
```

```javascript
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 a 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>
## Prohibited keywords

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 in Edge Encryption**

Edge Encryption 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 then control several aspects of this separation, including which users can see and access data.

**Overview**

**Support: Data only**

Domain separation in this application is supported at the Data only level, meaning it supports the data security model of separating visibility of data from one domain to another. To learn more, 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.
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.
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 your proxy servers.

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
</table>
| Invalid Insert Attempts (sys_edge_encryption_invalid_insert) | List of attempts to save the following data to encrypted fields:  
  - Unencrypted data.  
  - Data that did not come from an Edge Encryption proxy.  
  The instance rejects and 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 (sys_encryption_job_execution) | A list of jobs that did not execute successfully.                                                                                                                                                                                                                                                                                           |
| 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 following properties.
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>edgeencryption.stat.collection.enabled</td>
<td>Enables the collection of statistics used by the Edge Encryption proxy server performance dashboard.</td>
</tr>
<tr>
<td></td>
<td>• Default value: true</td>
</tr>
<tr>
<td></td>
<td>Add this property and set the value to false to disable the collection of statistics used by the Edge Encryption proxy server performance dashboard. After adding proxy server performance properties, you must restart the proxy server for the change to take effect.</td>
</tr>
<tr>
<td>edgeencryption.stat.collection.interval</td>
<td>Interval length in seconds during which the Edge Encryption proxy server collects statistics. The value cannot be less than 30 seconds.</td>
</tr>
<tr>
<td></td>
<td>• Default value: 30</td>
</tr>
<tr>
<td></td>
<td>After adding proxy server performance properties, you must restart the proxy server for the change to take effect.</td>
</tr>
</tbody>
</table>

3. Restart the proxy server.

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>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.

The 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

This list view displays the log entries 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 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>Message</td>
<td>System-generated message regarding the nature of the occurrence. For example, the source of the occurrence might be EMAIL or Memory.</td>
</tr>
<tr>
<td>Source</td>
<td>Name of the process or area affected by the occurrence. For example, the source of the occurrence might be EMAIL or Memory.</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 application activity for an instance.

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>Created by</td>
<td>The user who created this activity.</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>
</tbody>
</table>
Client transaction timings

The Client Transaction Timings plugin enhances the system logs by providing more information on the durations of transactions between the client and the server.

By providing information on how time was spent during the transaction, performance issues can be tracked down to the source by seeing where the time is being consumed.

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 module Client Transactions to the System Logs application, which provides a list of every logged transaction between client and server within the last day. The following information is tracked:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created</td>
<td>The moment the transaction was recorded.</td>
</tr>
<tr>
<td>Response Time</td>
<td>The number of ms spent by the server in fulfilling the transaction.</td>
</tr>
<tr>
<td>Business Rule Time</td>
<td>The number of ms spent by business rules triggered by the transaction.</td>
</tr>
<tr>
<td>SQL Time</td>
<td>The 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>The number of ms spent by the network the client is connecting through.</td>
</tr>
<tr>
<td>Browser Time</td>
<td>The 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>The number of ms spent executing ui policy</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Type</td>
<td>Type of transaction (one of Form, List, Other)</td>
</tr>
<tr>
<td>Table</td>
<td>The table that was displayed e.g. incident, change_request</td>
</tr>
<tr>
<td>View</td>
<td>The 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order</td>
<td>The order during the load that this operation occurred</td>
</tr>
<tr>
<td>Type</td>
<td>The 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 particular 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>
</tbody>
</table>
| Queue count | Number of times that the system tried to send the push notification. The status of the push notification relates to its queue count.  
  - If the queue count is 0 for longer than expected, then there are no scheduled jobs that are trying to send the push notification.  
  - 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.  
  - If the queue count reaches 10, the system stops trying to send the push notification. The Type changes to failure. |
| Request ID  | 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. |
### 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.

The following fields can be included in the layout of the system log and any of the system mailboxes:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mailbox</strong></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><strong>State</strong></td>
<td>The current state of the email (Error, Ignored, Processed, or Ready).</td>
</tr>
<tr>
<td><strong>Receive type</strong></td>
<td>The type of inbound email (None, Forward, New, or Reply).</td>
</tr>
</tbody>
</table>
| **Type** | The status of the email. Choices are:  
- received: The server received this email.  
- 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 Error String field for details.  
- send - failed: The server has attempted to send the email and failed. See the Error String field for details.  
- 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 Error String field for details.  
- 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.  
- sent: The email was sent by the instance without any errors or issues. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>
| User                       | The name of the user, from the user record, of the instance from which the email notification was sent.  
Note: This is a string field. |
| Notification Type          | The type of notification. Choices are:  
• None  
• SMS  
• SMTP |
| UID                        | The unique ID of the email stored on the server.                                                                                           |
| Created                    | The date and time of the email activity for the locale of the machine running the instance.                                                |
| Deleted                    | For inbound email, indicates whether the email was deleted from the email server.                                                           |
| Weight                     | The weight of the email, which determines the sending priority relative to other notifications on the same table.                        |
| Importance                 | An indication that the email was sent with a changed level of importance, such as Urgent.                                                    |
| Originating Event and Notification | For emails generated by notifications, an embedded list that stores the event and notification that created the email.              |
| Subject                    | The email subject. For notifications, you create the subject text in System Notification > Email > Notifications.                         |
| Error String               | 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. |
| Recipients                 | The email addresses of the recipients.                                                                                                     |
| Body                       | 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.        |
| Content type               | The email content type.                                                                                                                    |
| Headers                    | Any headers embedded in the email.                                                                                                           |

**Event logs**

The event log records all system events that occur within the system.

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>

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:

Import log

<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.

© 2019 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.
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>
<tr>
<td>Target Name</td>
<td>The name of the element that was altered.</td>
</tr>
<tr>
<td>View</td>
<td>The view of the form that was altered if it was a form layout change.</td>
</tr>
<tr>
<td>Payload</td>
<td>The XML contents of the record after the change.</td>
</tr>
<tr>
<td>Remote Update Set</td>
<td>A reference to that update set if the change was performed by a remote update set.</td>
</tr>
<tr>
<td>Local Update Set</td>
<td>The update set the change is associated with.</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:

<table>
<thead>
<tr>
<th>Common log archive schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
</tr>
<tr>
<td>Event (ecc_event)</td>
</tr>
<tr>
<td>Queue (ecc_queue)</td>
</tr>
<tr>
<td>Event (sysevent)</td>
</tr>
<tr>
<td>Log (syslog)</td>
</tr>
<tr>
<td>Transaction Log</td>
</tr>
<tr>
<td>(syslog_transaction)</td>
</tr>
<tr>
<td>Email (sys_email)</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:

<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>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.
Index

A

access account
  LDAPS 1165
access control 1392
access controls 1392
ACL 1392
ACLs
  configuration watcher
    execution plan 1418
    using 1419
  controlling whether script conditions apply to reference fields 1412
  creating ACL rules 1402
debugging 1413
evaluate the admin override at the access level 1412
explicit roles 1423
hasRoles() 1411, 1423
internal and external users 1423
mandatory roles 1411
provide access to users 1411
snc_internal 1411, 1423
troubleshooting 1416
Activate fiscal calendar 674
activate plugins 7, 114
activated by maint 115
active directory application mode (ADAM)
  access account 1165
  backup 1163
  configuring 1159
  console 1160
  container 1161
  create objects 1161
delegation 1161
dependencies 1158
group objects 1161
instance 1159
LDAPS 1163
LDAPS certificate 1164
LDAPS connection 1165
objects 1161
organizational unit 1161
permission 1161
public key &certificate 1164
recovery 1163
redundancy 1163
security 1158
testing 1162
troubleshooting 1162
user objects 1161
userproxy objects 1161
Active Directory Federation Services
  creating a SAML logout 1215
  identity provider 1208, 1208, 1210, 1210, 1210, 1210, 1215, 1215, 1216
Active Directory, configure SSL access 1170
active transactions
  killing 1299
  viewing 1299
activities list
  customize 416
activity formatter
  add to a form 415
  create 415
e-mail property 418
  live feed 415
  security 413
activity stream
  max entries 426
ADAM
  ADAMSync 1165, 1166, 1166, 1167, 1168
  configuration file 1167, 1168
  configuring 1159
dependencies 1158
  example 1168
  instance 1159
  security 1158
  set up 1166
  user accounts 1166
add
  field
    table 557
add role
  existing role 1065
adding
  new department 1047
  suggestion fields 551
ADFS 1208, 1208, 1210, 1210, 1210, 1210, 1215, 1215, 1216
  See also Active Directory Federation Services
administrator
  table administration
    unique record identifier 837
    unique record identifier 837
Administer
  servicenow. 7
administration 7
Advanced Reporting
  database views 326, 327, 328, 331, 332, 332, 332, 334, 334
  metric definition support 1263, 1264, 1265, 1266
AES 128
  configure 1660
  encryption key 1660
AES 256
  configure 1662
  encryption key 1662
altiris integration 1025
annotate
  forms 405
  annotate forms 405
application development 1003
application quotas
  property 1341
  rules 1342

© 2019 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.
Application Usage Overview 1084
applications
  create a custom table 219, 224
apply ACLs
  AJAXGlideRecord 1412
approval summarizer
  formatter example 423
attachment
  configuring
    icon 410
  disabling
    table 409, 779
    file size limiting 408
    file types 777
    icon
      configuring 410
      table
        disabling 409, 779
        viewing 406
attachments
  administering 406
  restrict file extensions 408
  hide attachment (view) link 410
audit roles 1409
audit roles table
  sys_audit_role 1081
auditing
  reference fields 1499
authentication
  multifactor
    activating 1246, 1249, 1251
    configuring 1247
    disabling for a user 1249
    disabling on user table 1253
    disabling on your user profile 1253
    logging on 1251
    requiring for a user 1249
    two-factor 1244, 1248
auto-upgrade 1697
auto-upgrader 1697
B
backup
  active directory application mode (ADAM) 1163
  ADAM 1163
Base System Roles
  special administrative roles 1071
Blacklist IP Addresses 1711
breadcrumbs
  restricting 356
  suppressing 356
Breadcrumbs
  restricting 353
browser support
  list v3 373
C
calculated price fields 631
calendar
  schedule 688
Calendars
  creating 671, 673
certificate
  certificate authority (CA) 1468
  configure 1659
  generate with keytool 1468
  https 1659
  trusted server 1469
  upload 1468
certificates
  LDAP client 1467
  mutual authentication 1467
child record 429
choice list
time zone 732
choice list state field 466
CI changes 1496
CI relationships and history 1499
class
  base 207
  child 207
  parent 207
Client Transaction Timings 694, 695, 696, 1754
cmdb ci changes 1496
company name
  normalization 1263
complexity limits
  joins 206
computer telephony integration 1031
condition count widget
  add 474
configuration 7
configure group types
  assignment groups 1060
Configure properties 1385
configure transaction quota rule 1337
configuring
  attachment
    icon 410
  icon
    attachment 410
  suggested text
    journal fields 553
    string fields 552
configuring lists
  list calculations 338, 379
connection
  LDAPS 1165
  testing 1165
connection test module
  creating 1330
container
  ADAM 1161
  create 1161
content management 7
context menus
  action script 372
  create 368
  dynamic actions script 372
  onshow script 373
context ranking
  definition, creating 362
  list, ranking 364
  plugin, activate 361
  scrum ranking 366
  sort order, apply 365
  update sets 362
contextual search
  add functions 787
  define search context 787
  defining 787, 787, 797
  installed components 816, 818, 819, 821, 822
  record producer 797
  table 789
Contextual Search
  administering 812
  Administering 810
  configure properties 811
  Defining 792, 794, 795, 799
  installed components 816, 818, 823
  query feedback 815
  Roles 803
  This Helped 815
contextual security
  configuring 347
  Contextual Security: Role Management V2 1408
  Contextual Security: Role Management V2 REST API 1408
Contextual Security: Role Management V2 1409
  conversions 1345
Core configuration 7
Core Configuration
  List Administration 336
  overview 641
  Platform Performance 1268
  time 665
corrupt index
  regenerating 773
custom tables
  delete 227
  customized objects
  during upgrades 1349
D
data 7
data archiving
  affected records, verifying 847
  archive rule, setting 842
  archive schedule, changing 851
  archived strings, language of 847
  creating rules 843
  plugin 841
  related records 844
  restored records, archiving 852
  restoring 851
  viewing 849
data destruction
  creating rules 848
Data Dictionary Tables
  system dictionary 292, 294
data import
  schedule 951
  scripting options 953
Data Lookup and Record Matching Support
  create a custom data lookup table 618
  create a data lookup module 623
  create custom data lookups 618
  data lookup definition record 620
  data lookup table 619
  data lookup value 619
  troubleshooting 624
data management 835
data policy
  installed with 611
Data policy
  converting to a UI policy 616
  creating 612
  debugging 617
  fields 615
data preserver
  SAML properties 1001, 1176
data source
  choice list 899, 901
  create 902, 1131
Data Sources
  Custom CSV files 891
  File 887
  FTP extended properties 895
  JDBC 896
  LDAP 904
database 1084
Database Rotation 1007, 1009
database size 1084
Database Views
  add a table 328
  create a database view 327
  database views in the base system 334
  relabel a column 332
  specify a field to return 331
  specify number of records to return 332
  test the database view 332
  use disjunctions in complex queries 334
date and time fields
  configuring for the list editor 667
  personalizing the date format 667
  personalizing the time format 667
Date and Time Fields 665, 669, 669, 669, 670, 670, 671
daylight saving time
  time zone 730
default currency fields 629
default sort sequence
  list 343
define client scripts 452
delegation
  active directory application mode (ADAM) 1161
  ADAM 1161
delete
  custom tables 227
deleting all records
  table 227
dictionary attributes 302
dictionary override
  define 293
dictionary overrides 293
Did You Mean?
  suggestions, configuring 752
digest token authentication
  enabling exit script 1240
disabling
  attachment
    table 409, 779
drag-and-drop 408
  feature 408
table
  attachment 409, 779
Discovery
  SCCM
    Asset Intelligence scheduled imports 1023
    SCCM integration
      switching versions 1023
disposition
  upgrade history 1346
Document ID Field 478
document scoring 764
domain separation
  activating and deactivating domains 1584
  activating plugins 1574
  adding to a domain field 1584, 1590
  adding to a visibility domains list 1589
  applications 1513
  changing domain visibility 1589
  configuration module 1575
  creating contains relationships between domains 1589
  creating domain-specific choice lists 1591
default domain scope 1578
deprecated administration
  example with domain specific applications and modules 1600
  example with domain specific policies 1605
domain assignment 1503
domain query methods 1512
domain scope 1509
domain selection menus 1591
domain visibility 1506
  enabling domain logging and debug messages 1612
  enabling the domain reference picker on UI15 1592
  enabling the domain reference picker on UI16 1591
  granting visibility domains to a group 1584
  granting visibility domains to a user 1590
  limitations 1513
  making a domain the default 1581
  manage MSP domains for records 1583
  properties 1578
  re-enable domain separation 1598
  re-enabling delegated administration 1612
  restricting access by role 1594
  selecting a primary domain 1579, 1587
  setup 1574
  user preferences 1578
  validating domain hierarchy 1595
  viewing historical messages 1613
  viewing MSP domain relationships 1587, 1598
  viewing real-time messages 1612
  viewing tables that use domain separation 1598
Domain separation 1591
  domain separation for MSPs
    activating and deactivating domains 1584
    changing domain visibility 1589
    creating a domain 1579
    installed components 1518
    making a domain the default 1581
    manage MSP domains for records 1583
    selecting a primary domain 1587
    viewing MSP domain relationships 1587, 1598
    domain separation for schedule 689
domain separation setup 1581, 1584, 1598, 1613
domain support 689
  drag-and-drop
    disabling 408
    feature 408
dynamic creation 522
E
e-signature approval
  SAML 2.0 authentication, setting up 1109
Easy Import
  add a record in the template 975
data type validation 981
  import a record from the template 977
  import template 974
paste data into the template 979
template type validation 981
template validation 979
update a record in the template 976

Edge Encryption
adding proxies 1680
attachment decryption job 1708
attachment encryption 1707
attachment encryption job 1707
attachment key rotation job 1703
attachments 1707
configuration 1701
configure 1745
configuration attributes 1739
digital signature 1669
encryption application 1634
ecnryption change 1709
ecnryption deactivation 1704
ecnryption job 1705
ecnryption key management 1635
ecnryption patterns 1709
ecnryption proxy 1634
ecnryption rule actions 1720
ecnryption rule conditions 1719
ecnryption rules 1716, 1719
ecnryption type
  change 1709
deactivate 1704
ecnryption types 1637
field encryption 1704
file store 1675
getting started 1644
installation 1652
installed components
tables 1639
installer 1653, 1654, 1659, 1660, 1662, 1663, 1665
instance configuration 1703
Java Cryptography Extension (JCE) installation 1670
Java KeyStore 1672
java.security policy file 1671
key management 1635, 1675
key rotation 1675, 1701
key store management 1635
keytool utility 1672
limitations 1649
Linux installation 1667
Linux uninstall 1681
Linux update 1699
mass encryption jobs 1710
mass key rotation job 1702
NAE key store 1673
order token repair job 1710
overview 1631
password encryption 1680
patterns 1637
prohibited keywords 1739
properties 1677
proxy download 1653
proxy properties 1684
proxy system requirements 1645
proxy update rollback 1700
proxy upgrade 1693
secure SSL connection 1669
set up encryption key 1671
set up keystore 1671
single key rotation job 1701
start the proxy 1663, 1665, 1679
stop the proxy 1681
user account 1653
web proxy configuration properties 1677
Windows installation 1667
Windows uninstall 1682
Windows update 1700

Edge Encryption environment
memory 1648
Number of proxy servers 1648
redundancy 1648

email
  notifications
    events
      business rules 827
      creating an event 832
      global 831
      passing parameters 834
      reprocessing 834
      states 824
      using a business rule 825
embedded lists
  securing records 1406
  within a form 399
embedding
  HTML fields
    images 493
  images
    HTML fields 493
employee self-service
  login scenarios 1439
enable auditing
  table 1485, 1485, 1486
Encrypted field configuration 1623
Encryption
  support 1617, 1621, 1622, 1625, 1625, 1630
Encryption Context 1620
encryption proxy
  adding proxies 1680
  digital signature 1669
  download 1653
  encryption key management 1635
  file store 1675
  installer 1653, 1654, 1659, 1660, 1662, 1663, 1665
  Java Cryptography Extension (JCE) installation 1670
  Java KeyStore 1672
  java.security policy file 1671
  key management 1635
  keytool utility 1672
  Linux installation 1667
  Linux uninstall 1681
Linux update 1699
NAE key store 1673
password encryption 1680
properties 1684
scheduled upgrade 1693
secure SSL connection 1669
start the proxy 1663, 1665, 1679
stop the proxy 1681
system requirements 1645
update rollback 1700
web proxy configuration properties 1677
Windows installation 1667
Windows uninstall 1682
Windows update 1700
encryption scripting 1628
Encryption Support 1623
enter submits form
   change preference 454
entity generation 711
escalation intervals 706
event log 823
event queue 823
event registry 714, 824
events
   schedule 714
Export Data
   break up a large export 874
   enable export debug logging 875
   export directly from the URL 870
   export form data 858
   export limits 855
   export list data 859
   export list fields 860
   filter list result 861
   url export 872
   url query 861
Export public key certificate 1172
Export set
   Schedule an export 879
Export sets
   Cancel an export 883
   create an export definition 878
   Create an export target 879
   create new 877
   easy export 878
   History 882
   scheduled export
      scripting 881
Export Sets
   properties 883
Exporting data
   Exporting currency fields to Excel 869
Exporting Data
   export data 854, 855, 858, 859, 860, 861, 870, 872, 874, 875
Express conversion to Service Management 1378, 1378, 1379, 1380, 1381, 1382
   extend 216
External Authentication (Single Sign-On - SSO) 1196, 1198, 1202, 1216, 1220, 1253

F

feature
disabling 408
drag-and-drop 408
field
   add spell checking 505
   creating
      new 557
field administration
   choice field search 473
   choice fields 473
Field Administration
   choice lists
      change none display value 470
      customize 463
      define option 468
      delete 471
      field type 472
      remove none option 469
      reuse 468
      security 464
create a wikitext field 555
data lookup and record matching support 618, 618, 618, 619, 620, 623, 624
default choice lists
   integer values 465
   extend functionality of a wikitext field 556
   field normalization 573, 575
   reference fields 523, 523, 525, 526, 527, 527, 529, 529, 532, 532, 533
   supported wiki tags 554
   use phone number fields 509, 509, 509, 509, 509, 510, 510, 511, 512, 513, 514, 516, 518, 520, 520
   values associated with choices
      scripting 464
      wiki fields 554
Field map
   Script variables 947
Field Normalization
   installed with 575
Field Normalization Rules
   expressions 608, 610
   patterns 608, 610
Field Styles
   defining 562, 564
field transformations
   create transformation records 597
   run data jobs 583, 583
   select transform types 598
   test 599
field type
   create 578
fields
   HTML fields
      HTML sanitizer 1478, 1481, 1481, 1482, 1482
Fields
   creating new 557, 556, 557, 568
   introduction 564

© 2019 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.
file
  attachment 408
  role 408
file size
  attachment limiting 408
filter out
  hidden groups 1060
filter potential assignees
  based on skills 1063
filters
  related list query blacklist 378
  restricting 356
  suppressing 356
Filters
  restricting 353
Financial Management
  fiscal calendar 674
fiscal calendar
  generate 675
  view fiscal periods 677
fixed price fields 631
form administration
  create a UI policy 448, 448, 616
  create a UI policy example 451
form design 382, 388, 388, 388, 390, 390
form annotations
  add 392
  language support 405
  toggle 394
  types 405
form design
  add a formatter 390
  add annotation 388
  display field 388
  new field 390
  new section 388
form personalization
  activate 404
  administer 403, 404
  disabling 405
  manage 404
  role requirements 404
  user preferences 404
form section
  create 395
form splits
  add property to enable 454
form submission
  double-check 1410
form templates
  automatically applied 427
  create from form 427
  save form as template 433
  scheduling 435
  template bar 437
formatter
  approval summarizer 423
  create 412
  create UI macro 411
  override with macros 425
forms
  activity formatter
    live feed 415
  add activity formatter 415
  adding charts 401
  adding related lists 392
  annotate 405
  configure 390
  configure condition builder 475
  configure customer updates indicator 401
  configure insert for task records 453
  control the label type 458
  customize activities 416
  define required fields 457
  personalize 403, 404, 404, 404
  personalizing 405
  use HTML fields 488
frequency 779

G
general security settings
  properties 1420
Generate a certificate 1171
Glide
  durations format
  modifying 321
glide.history.role 1496
global
  print(String message) 1738
Global Catalog 1173
global text search
  search field 737
  search groups 744
  search preferences 749
  search result groups 737
  search suggestions 752
Google
  activating plugin 1014
grant role access
  applications 1065
  modules 1065
group skill
  assign 1062
group type
  add 1061
  assign 1061
groups
  add a user 1059
  create 1058
  hide 1060
  remove a user 1059

H
hidden field
  group form 1060
hidden groups
  filter out 1060
hierarchical list
  enable 358
high security settings
activating 1437
default deny property 1410
elevated privilege 1425
elevating to a privileged role 1428
forcing administrators to manually elevate 1429
history access
control 1488
history calendar 1492
history list 1489
history sets
comparing CI snapshots 1499
differences with audit 1488
export historical CI snapshot 1498
HTML editor
paste options 497
HTML fields
embedding
images 493
video 495
image uploads 497
images
embedding 493
linking
website 494
TinyMCE deprecated tags 481, 482
TinyMCE HTML editor 479
TinyMCE HTML toolbar 479
video
defining file types 496
embedding 495
website
embedding 494
HTML Fields
TinyMCE version 4 editor 488
HTTP 500 error 204

I
icon
attachment
configuring 410
configuring
attachment 410
Identity provider
Active Directory Federation Services 1208, 1208,
1210, 1210, 1210, 1215, 1215, 1216
IdP 1208, 1208, 1210, 1210, 1210, 1215, 1215, 1216
See also identity provider
Image fields
using 497
Images
embedding
HTML fields 493
HTML fields
embedding 493
Impersonate a User
force logout 1056
log impersonations 1055
on a mobile phone 1053
import data using import sets
Perl example 954
post CSV or Excel files directly to an import set 953
review the import set 948
run import 948
Import log
viewing 949
Import run history 950
Import Set Performance
troubleshooting 982, 983, 983, 983, 984, 984, 984,
984
import set tables
web services 1029
import sets
performance improvements 1299
Import sets
Importing data using import sets 929
maximum row size 929
Import Sets
Coalesce 920
easy import 973, 974, 975, 976, 977, 979, 979, 981,
981
properties 955
web proxy 213, 214, 215, 215
Import sets properties 955
importing
XML records 985
Importing
ServiceNow instance 985, 986, 987, 988, 988
XML records
matching existing records 986
inactivity monitors
setting 706
index
field, removing 774
HTML 769
removing 774
index suggestions for slow queries
export to non-production instance 1289
generate 1285
review 1286
schedule index creation 1290
schedule index drop 1295
test index performance 1294
indexing 770, 777
install edge encryption 1667
installation exits 1442
Instance
translate 659, 659, 660, 660, 661, 661, 661, 662, 663,
663, 664, 664, 664
Instance locale
set 641
Instance Security Dashboard 1385
Instance Usage 1084
Integrate
1010
Integrate
Edge Encryption 1741
integration 1010, 1741
Integrations
available 1011
Internal CA, generate certificate 1171
internationalization
support 642
Introduction to Fields
change 558
character counter 504
database field types 476
delete 559
delete multiple 559
field label 558
hint 558
IP address field type 498
text field 504
types 459
IP Range Based Authentication
access control 1457
block a particular range 1457
block everyone except a particular range 1457

J
Java digest algorithm
encryption 1242
JDBC driver
choice list, edit 899, 901
data source, create new 902
DB2 901
Install on a MID server 902
Sybase 901
JDBCProbe 1035, 1035, 1036, 1037, 1038, 1040
job
schedule 712
journal fields
configuring
suggested text 553
JSON API 1733
JsonNode
encodedQueryFor(String tableName) 1737
getAsString() 1736
getAsString(String propertyName) 1736
getIterator(String xPath) 1735
getName() 1737
iterator() 1736
valueFor(String tableName, String fieldName) 1737
JsonNode API 1735
JsonNodeIterator
hasNext() 1738
next() 1738
JsonNodeIterator API 1738

K
keyword search 779
knowledge
incident deflection and resolution 803
Knowledge
Incident Deflection and Resolution 804, 808, 811

L
language internationalization support
Choices table 648
configure a language as reading from right to left 645
Field Label table 647

LDAP
Active Directory 1140
assign field values 1141
binary data through mid server 1134
BLOB data 1134
common scripts 1140
connection monitoring 1133
create server 1119
deactivate 1140
exclude users 1141
extraction 1155
filters 1154
import maps 1135
inactive accounts 1156
integration
error codes 1146
troubleshooting 1142
listener
setting up 1125
MID Server
troubleshooting 1134
notifications 1133
one-time password 1154
organizational unit 1129
OU 1129
refresh 1142
schema 1174
script 1140, 1141, 1141
script examples 1156
setup 1117, 1133
specifying attributes 1127
SSL certificate 1119
testing connections manually 1128
transform map 1136, 1142
user account
deactivate 1156
disabled 1156
user auto provisioning 1132
verify mapping 1142
X.509 certificate 1119
LDAP Connection Failed 1133
LDAP Monitor
view 1144
LDAP records
inactive 1154
synchronize 1154
LDAP transform
choice action 1142
create 1142

© 2019 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.
ignore 1142
reject 1142
LDAPS
ADAM 1163
certificate, assigning 1164
connection 1165
public key certificate 1164
self-signed certificate 1163
left-pad numbers
in custom tables 571
limiting
attachment
file size 408
file size
attachment 408
Linux 1680
Linux stats 1324
list administration
list v3
disable for a table 381
disabling globally 380
enabling for related lists 380
list calculations 338, 379
list control 342
list control settings
for list editor 346
list controls 338, 342
list editor
administering 344
contextual security, configuring 347
control settings, configuring 346
user preferences, managing 351
list editor properties
configure editable field types 345
disable list editing 345
list mechanic
access, controlling 352
activating 352
list v3
browser support 373
compatibility 374
debug compatibility 374
installed components
properties 375
lists
detail rows
enabling 353
locales
define 641
localization
form annotations 405
system 657
Localization
instance 659, 659, 660, 660, 661, 661, 661, 662, 663, 663, 664, 664, 664
localization properties 657
location setup 659
Login
finding denied IP addresses 1458
IP range based authentication 1456, 1457, 1457, 1457, 1458
login landing page
specifying 1440
Login Scenarios 1438
login security
activating ServiceNow access control 1464
configuring ServiceNow access control 1465
ServiceNow access control 1462
logout button
remove 1442
logout confirmation prompt
enable 1441
M
Managing Data
system clone 990, 993, 995, 996, 999, 1005, 1006
manually install
proxy server 1667
Many to Many Task Relations
define a relationship type 285
define a task relationship allowed 286
mark as solution button 287
modify the displayed field 287
plugin manifest 284
request the plugin 284
task relationship type record 286
ui actions 287
many-to-many relationship
creating 325
referencing 326
match relevance by
field, controlling 766
Metric Definition Support
metric definition 1264
metric instance 1266
sample field value duration script 1265
metric definitions 729
Microsoft
SMS/SCCM integration 2.0 1015
Microsoft Active Directory, configure SSL access 1170
Microsoft SCCM
configuration 1020
schedule 1020
MID Server
configure 1745, 1745
integrate Edge Encryption 1745, 1745
modify form focus 453
multi-tenancy 1500, 1501, 1513
multiple fields
sort 344
multiple price fields 631
Multiple Provider
single sign-on
using with ESS 1108
Multiple provider SSO 1682
MySQL global status 1316
N
navigation and UI
context menu 368, 372, 372, 373
new customizations
  translate 651
new department
  adding 1047
Non-Interactive Sessions 1082, 1083, 1083, 1083, 1083
Nonce
  implementing 1458, 1459, 1459
normalization
  company name 1263
  properties 1262
Normalization Data Services 1263
number of history entries
  change 1489

O
OAuth
  activating 1224
  APIs
    scoped 1238
  authorization code flow 1232
  authorization code grant flow 1232
  authorize access 1235
  external client scenario 1225
  manage OAuth tokens 1237
  profile
    parameters 1228, 1229
    property 1224
    revoking a token 1238
    setting up 1223
OAuth 2.0
  authorization code flow
    instance as authorization server 1236
ODBC Driver 1741, 1743
ODBC truststore 1743
on load check box 452
OpenLDAP
  modify 1174
order-preserving database 1663
Order-preserving encryption 1649
organizational unit
  ADAM 1161
  create 1161

P
pages
  make public 1441
parallel processing
  configuring 747
ParameterValue
  encodedQueryFor(String tableName) 1726
  toString() 1725
  valueFor(String tableName, String fieldName) 1726
parent record 429
password reset
  notification 1448
Password Reset
  properties 1448
  user lockout 1440
password validation rules
  strengthen 1444
pause conditions 706
Percent Complete Field 507, 507, 508
performance
  evaluating 1277
performance metrics
  AMB graphs 1320
  database graphs 1312
  Discovery graphs 1314
  MySQL global status graphs 1316
  replication throughput 1312
  slow pattern graphs 1318
Performance Metrics 1322
personal lists
  administering 352
  managing 352
personalizing lists
  list calculations 338, 379
Personalizing Lists 342
Planned Task 248, 248, 249, 250, 251, 252, 254
Planned Task Hierarchy 253
Platform encryption 1620
Platform Performance
  Stats Tools plugin 1277
  table extension 1344
  troubleshoot performance 1268, 1269, 1271, 1273
Platform security
  overview 1384
Plugin
  Google custom search integration 1014
plugins
  activate 7
  general 114
  options for activating 114
  purchase 115
Plugins
  List of Plugins 8
pop-up information
  customize 531
Portal
  Time Sheet 262
  preserve applications 1003
  price fields 631
  process flow formatter
    activating 420
    create 420
Production System 1025
properties
  base system 123
  properties module
    creating 203
proxy database 1663
Proxy database
  size 1649
Proxy Error Reports 1745
Proxy performance dashboard 1745
proxy server
  set initial memory 1678
  set memory 1678
  set upper bound memory 1678
proxy server installation 1667
public key certificate
  exporting 1164
LDAPS 1164
Public key certificate, export 1172
punctuation 767
purchase plugins 114, 115

Q
query method
   configuring 747
query mode
   single table 774
quotas
   application 1341
   application properties 1341
   transaction 1333

R
range calculator scripts 703
ranking
   stories 367
read only role 1072
read-only fields
   pop-ups 531
record
   deleted 1175
Record Numbering
   managing 569, 570, 572, 573
record producer 806
records lists
   enable text searches 769
   text searches 753
recovery
   active directory application mode (ADAM) 1163
   ADAM 1163
redundancy
   active directory application mode (ADAM) 1163
   ADAM 1163
reference autocompletes
   using wildcards 549
reference currency 629
Reference Field
   auto-complete 541
reference fields
   add 522
   dynamic creation 522
   recent selections 550
Reference Fields
   auto-complete 524, 543, 544, 545, 546, 548
   cascade delete rules 523
   decorations 527
   define reference key 523
   display values 525, 526
   lookup 527, 529
   reference icon 529
   reference styles 533
   related incidents icon 532
   select 526
   show workflow icon 532
   tree picker 529
   reference qualifiers 533, 538, 539, 540, 541
registering
   event 715, 833
related list
   select 360
related list query
   blacklist system property 378
related lists
   enabling list v3 380
related record 429
related tables 216
relative duration
   define 697
   use 698
Remember Me check box
   default value, changing 1456
   removing 1456
reminder 254
request
   getAsJsonContent() 1721, 1725
   getAsXmlContent() 1722, 1725
   XMLContains(String path) 1722
request API 1721
request plugins 114
resolve conflicts 1349, 1356
restore deleted records
   configure 1486
   deletion audit 1486
   system table 1486
restoring deleted records and references 232
restrict a field
   example 348
   with a condition, example 350
   with a script, example 349
restrict a table
   example 347
role
   attachment
      file 408
      file
   attachment 408
role delegation
   prevention 1075
roles
   acl rules 1076
   create 1064
   group
      assign role 1065
      creating 1065
   security jump start 1076
Roles
   base system roles 1066, 1071
   RSA key pair 1659
S
SAML 2.0
   Java keystore 1190
   profile 1099, 1103, 1175, 1178, 1179, 1180, 1180, 1180, 1181, 1181, 1182, 1183, 1183, 1183, 1184, 1184, 1184, 1185, 1185, 1185, 1186, 1190, 1191, 1191,
spans 727
spell checking
  add to a field 505
SSL access, configure Microsoft Active Directory 1170
stand-alone CA, set up 1171
Standard Import Set Tables 922
statistics
  text indexing 775
Stats Tools
  performance evaluation 1277
status
  text indexing 775
stop words
  automatic, configuring 781
  global, configuring 780
  table-specific, configuring 780
stories
  ranking 367
string fields
  configuring
    suggested text 552
suggestion fields
  adding 551
Support
  encryption 1617, 1621, 1622, 1625, 1625, 1629
supported interfaces 1031
synchronize
  LDAP records 1154
synonym dictionaries 784
synonym dictionary 784
synonym search
debug 785
sys audit table
  understanding 1484
syslog probe 1043
system clone
  SAML integration 1001, 1176
System clone
  exclude a table from cloning 996
  start a clone 993
System Clone
  create a clone target 995
  preserve data 999
  run post clone cleanup scripts 1006
  view active clones 1006
  view clone history 1006
system diagnostics
  running 1273
system dictionary
  modifying 294
System Dictionary
  dictionary entries 294
system localization 657
system log messages 1340
system logs
  restore deleted records 1486
system properties
  adding 201
System Scheduler 707

T

tabbed forms
  display 397
table
  attachment
    disabling 409, 779
    viewing 406
  contextual search 789
deleting 227
disabling
  attachment 409, 779
  extending 207
table administration
  restoring deleted records and references 232
  unique record identifier 838, 838, 838
Table Extension
  example 1344
table field
  prevent auditing 1486
table hierarchy
  extension model 1329
table index 234
table rotation
  apply 1326
tables
  delete 227
Tables
  schema map 322, 322, 323
tables module 225
task parent breadcrumbs formatter
customize 422
task table
  flattening 1328
Task table
  activate time cards 256
  copy time cards 278
  creating a task 234
  Important Task table fields 242
  journal fields 245
  modifications 255
  modify the task interceptor 247
  Planned Task plugin 234
time cards 255, 275, 275, 280, 281
time sheet policies 257
time sheets 272
tools for driving tasks 282
Task Table
  assignment lookup rules example 235
  assignment module rule 238
  assignment rules 237
  assignment rules module 236
  baseline assignment rules example 237
  business rules 237
  condition editor example 236
data lookup rules 236, 241
  defining assignment rules 235
  many to many task relations 283, 284, 284, 285, 286, 287, 287, 287
  workflow assignments 237

tasks
  tasks workflow 255
technical 7

template
   apply from a module 435
   scripting 438

Test LDAPS connectivity 1172
text index 770
text indexing
   statistics 775
   status 775
TF-IDF scoring 765
third-party 1010
this ServiceNow instance 1331
threads
   performance monitoring 1300
time
   display 699
   scheduled jobs 713
Time
   time zones 734
   view system logs 825, 1482, 1752, 1753, 1756, 1757, 1758, 1759, 1759, 1760

Time card
   submit time card 279
time card management
   time cards 255
time sheet policies 257
Time card management
   approve time sheet 274
   assign time sheet policy to a user 261
   create time sheet 272
   reject time sheet 274
   set time sheet policy as default policy 261
   submit time sheet 274
time cards 275
   Time Sheet Portal 262
time sheets 272
time cards
   approve time card 280
   reject time card 280
time sheet policies 257
time sheets 272

Time cards
   Time Sheet Portal 269

Time Cards
   auto generate time cards 278
   create time cards 275
   scheduled job 278
time sheet portal
   approve time sheet for your resources 271
   submit a time sheet for your resources 271

Time Sheet Portal
   Create time cards 269
   log time 269
   submit time sheet 271
time sheets
   approve time card 280
   approve time sheet 274
   approve time sheet for your resources 271
   assign time sheet policy to a user 261
   create time sheet 272
   create time sheet policy 257
   reject time card 280
   reject time sheet 274
   set time sheet policy as default policy 261
   submit a time sheet for your resources 271
   submit time card 279
   submit time sheet 274
time cards 275

Time Sheets
   copy time cards 278
   create time cards 275
time worked fields 730
time zone
   choice list 732
   scheduled data import 734
   scheduled reports 733
time zones
   daylight saving time 730
   email notification 730
   scripting 730
   service level agreement 730
   user preferences 730

Time-Related Functionality
   introduction 702

Timeline Pages 715, 717, 721, 721, 723, 724
timelines 727, 1496
Timelines
   using 727, 727
timing functionality 729

TinyMCE HTML deprecated tags 481, 482
TinyMCE HTML editor 479
TinyMCE HTML toolbar 479

Tokenization 1649

transaction
   cancel timer 1297
   canceling 1297
transaction quotas 1333

Transaction Quotas 1334, 1335, 1336, 1336, 1339, 1340

transactions
   canceled 1299
   logging 1299
   transform category
      create 608
   transform definitions
      create 604
   transform map
      create 935

Transform Map Scripts
   event scripts 912
   transformation script variables 908

Transform Maps
   creating 906, 938, 943
   translatable strings
      locate 651
   translate and learn property
      use 653

Translated Text 655, 656, 656, 656
translation prefix
   display 651

Troubleshoot Performance
   compression 1273
   network response times 1271
   response time on forms 1269

© 2019 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.
transaction log response times 1268
Type
  Rate 261
type ahead
    suggestions, updating 752
U
ui actions 343
Ui actions 439, 442, 444, 445, 447
Ui policies
  client scripts 452
Ui policy
  creating from a data policy 616
unique record identifier 837
untranslated string
  export 652
upgrade
  proxy server 1697
Upgrade History 1346, 1356
upgrade monitor
  upgrade platform 1357
  upgrade system 1357
Upgrade Monitor />
  upgrade instance 1357
upgrades 1345
Use HTML Fields
  editing functions 487
  extended functions 485
  formatting 483
  highlight text in the TinyMCE editor 491
  insert a line break 491
  style a table 491
Use Phone Number Fields
  configure e.164 phone number fields 509
  dependent fields 509
  display of local format 510
  e.164 phone number field dictionary attributes 516
  e.164 phone number field system properties 514
  entry of international format 510
  international direct dialing prefix 513
  phone formats 520
  phone territory selector choice list 511
  phone validations 520
  territories assigned 509
  territory format validation 509
  territory labels 512
  territory phone display rule 518
Use Time Zones
  set a system time zone 734
user 7
User administration
  company 1046
user preferences
  list editor, managing 351
user registration
  approve an account 1053
  enable auto processing 1045
user sessions
  locking out a user 1057
  making a user inactive 1057
  managing 1056
  terminating a user session 1057
User sessions
  modify session timeout 1056
user skill
  assign 1062
users
  allow to view a profile 1045
  assign roles 1066
  create 1048
Users and Groups
  impersonate a user 1053, 1054, 1054, 1055, 1056
Using Forms
  use HTML fields 479, 483, 485, 487, 491, 491
V
validation script
  deactivate 1050
Verizon
  eboning
    migrating 1025
  integration 1025
video
  defining file types
    HTML fields 495
  embedding
    HTML fields 495
  HTML fields
    embedding 495
view cmdb ci 1496
View System Logs
  audited tables 1482
  customer updates table 1759
  email logs 1756
  event logs 825, 1757
  import logs 1758
  log history 1759
  log utilities 1760
  system diagnostics application 1758
  system logs 1752
  transaction logs 1753
  viewing
    attachment table 406
    table
      attachment 406
  VPN communication
    create address 1617
  VPN service
    request 1617
W
watch lists
  configure email notifications 560
  configure order buttons 560
  hide email addresses 560
  use 559
Web Proxy
  ntlm authentication 214
  proxy servers 215, 215
  soap clients 215
Web service import sets 962, 966, 969
Web Service Import Sets
  Security requirements 970
web service security 1470, 1472, 1475
website
  HTML fields
    linking 494
    linking
    HTML fields 494
words 767

X
XML API 1726
XML files
  export 875
  import 875
XML Files
  exporting 853
  importing 853
XML import sets 986
XmlContent 1726
XMLContent
  getIterator() 1729
  getIterator(String XPath) 1730
XMLContent API 1729
XMLElement
  encodedQueryFor(String tableName) 1732
  getAttributeValue(String attribute) 1732
  getIterator(String XPath) 1731
  getIteratorOverAllChildren() 1731
  getName() 1732
  valueFor(String tableName, String fieldName) 1731
XMLElement API 1731
XMLElementIterator
  hasNext() 1730
  next() 1730
XMLElementIterator API 1730

Z
Zing
  junk filter, disabling 748
  text search, debugging 748
Zing text search 735